



CVE-2016-7958

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-7958
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-12 10:59:00 UTC
Updated	2023-11-07 02:35:00 UTC
Description	In Wireshark 2.2.0, the NCP dissector could crash, triggered by packet injection or a malformed capture file. This was addressed in Wireshark 2.2.2.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	2.2.0	All	All	All
Application	Wireshark	Wireshark	2.2.0	All	All	All

References

Reference	Source	Link
code.wireshark Code Review - wireshark.git/commit	CONFIRM	code.wireshark.org
Wireshark · wnpa-sec-2016-57 · NCP dissector crash	CONFIRM	www.wireshark.org
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org
Wireshark NCP Dissector 'packet-ncp2222.inc' Denial of Service Vulnerability	BID	www.securityfocus.com
12945 – CMake builds don't register the NCP dissector, so the resulting Wireshark/TShark crashes with NCP packets	CONFIRM	bugs.wireshark.org
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

[671108](#) EulerOS Security Update for wireshark (EulerOS-SA-2019-2425)

© [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](#)