



CVE-2020-25862

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

Summary

CVE	CVE-2020-25862
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-06 15:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	In Wireshark 3.2.0 to 3.2.6, 3.0.0 to 3.0.13, and 2.6.0 to 2.6.20, the TCP dissector could crash. This was addressed in epan

Risk And Classification

Problem Types: CWE-354

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
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Hardware	Oracle	Zfs Storage Appliance Firmware	-	All	All	All
Hardware	Oracle	Zfs Storage Appliance Firmware	-	All	All	All
Operating System	Oracle	Zfs Storage Appliance Firmware	8.8	All	All	All
Operating System	Oracle	Zfs Storage Appliance Firmware	8.8	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

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

References

Reference

[Wireshark · wnpa-sec-2020-12 · TCP dissector crash](#)

[ERROR:epan/proto.c:9868:hfinfo_number_value_format_display: code should not be reached \(#16816\) · Issues · Wireshark Foundation / wireshark](#)

[TCP: do not use an unknown status when the checksum is 0xffff \(7f3fe616\) · Commits · Wireshark Foundation / wireshark · GitLab](#)

[\[SECURITY\] Fedora 33 Update: wireshark-3.2.7-2.fc33 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 32 Update: wireshark-3.2.7-1.fc32 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 32 Update: wireshark-3.2.7-1.fc32 - package-announce - Fedora Mailing-Lists](#)

[\[security-announce\] openSUSE-SU-2020:1882-1: moderate: Security update for wireshark](#)

[\[SECURITY\] \[DLA 2547-1\] wireshark security update](#)

[\[SECURITY\] Fedora 31 Update: wireshark-3.2.7-1.fc31 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 33 Update: wireshark-3.2.7-2.fc33 - package-announce - Fedora Mailing-Lists](#)

[\[security-announce\] openSUSE-SU-2020:1878-1: moderate: Security update for wireshark](#)

[\[SECURITY\] Fedora 31 Update: wireshark-3.2.7-1.fc31 - package-announce - Fedora Mailing-Lists](#)

[Oracle Critical Patch Update Advisory - January 2021](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178650](#) Debian Security Update for wireshark (DLA 2547-1)

[199625](#) Ubuntu Security Notification for Wireshark Vulnerabilities (USN-6262-1)

[296071](#) Oracle Solaris 11.4 Support Repository Update (SRU) 27.82.1 Missing (CPUOCT2020)

[501328](#) 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](#).

