



CVE-2020-13164

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

Summary

CVE	CVE-2020-13164
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-19 22:15:00 UTC
Updated	2023-11-07 03:16:00 UTC
Description	In Wireshark 3.2.0 to 3.2.3, 3.0.0 to 3.0.10, and 2.6.0 to 2.6.16, the NFS dissector could crash. This was addressed in epan

Risk And Classification

Problem Types: CWE-674

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	31	All	All	All
Operating System	Fedoraproject	Fedora	32	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
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2020:1188-1: moderate: Security update f	SUSE	lists.opensuse

[SECURITY] Fedora 32 Update: wireshark-3.2.4-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[security-announce] openSUSE-SU-2020:1199-1: moderate: Security update f	SUSE	lists.opensuse.org
[SECURITY] Fedora 31 Update: wireshark-3.2.4-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org
16476 – Crash when opening given pcap; cycle in the directory graph indicated by NFS causes infinite recursion	MISC	bugs.wireshark.org
Wireshark · wnpa-sec-2020-08 · NFS dissector crash	MISC	www.wireshark.org
code.wireshark Code Review - wireshark.git/commit	MISC	code.wireshark.org
Wireshark: Multiple vulnerabilities (GLSA 202007-13) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] Fedora 32 Update: wireshark-3.2.4-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 2547-1] wireshark security update	MLIST	lists.debian.org
[SECURITY] Fedora 31 Update: wireshark-3.2.4-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.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

- [178650](#) Debian Security Update for wireshark (DLA 2547-1)
- [199625](#) Ubuntu Security Notification for Wireshark Vulnerabilities (USN-6262-1)
- [296074](#) Oracle Solaris 11.4 Support Repository Update (SRU) 22.69.4 Missing (CPUAPR2020)
- [501325](#) Alpine Linux Security Update for wireshark

© [CVE.report](https://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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report