



CVE-2021-22174

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

Summary

CVE	CVE-2021-22174
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-17 15:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	Crash in USB HID dissector in Wireshark 3.4.0 to 3.4.2 allows denial of service via packet injection or crafted capture file

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Oracle	Zfs Storage Appliance	8.8	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 33 Update: wireshark-3.4.3-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedor
[SECURITY] Fedora 33 Update: wireshark-3.4.3-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor
Wireshark · wnpa-sec-2021-02 · USB HID dissector crash	MISC	www.wire
2021/CVE-2021-22174.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.con
Buildbot crash output: fuzz-2021-01-18-1999268.pcap (#17165) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	gitlab.con
[SECURITY] Fedora 32 Update: wireshark-3.4.3-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedor
[SECURITY] Fedora 32 Update: wireshark-3.4.3-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor
Wireshark: Multiple vulnerabilities (CVE SA 202107 21) - Gentoo security	GENTOO	security.g

wireshark: multiple vulnerabilities (GLSA 202107-21) — Gentoo Security	GENTOO	security.g
Oracle Critical Patch Update Advisory - April 2021	MISC	www.orac
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179795 Debian Security Update for wireshark (CVE-2021-22174)
501718 Alpine Linux Security Update for wireshark
710055 Gentoo Linux Wireshark Multiple vulnerabilities (GLSA 202107-21)
750694 SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2021:2125-1)
750715 OpenSUSE Security Update for wireshark, libvirt, sbc, libqt5-qtmultimedia (openSUSE-SU-2021:0909-1)
750814 OpenSUSE Security Update for wireshark (openSUSE-SU-2021:2125-1)

© [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](#)