



# CVE-2021-22207

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

## Summary

<b>CVE</b>	CVE-2021-22207
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-23 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:30:00 UTC
<b>Description</b>	Excessive memory consumption in MS-WSP dissector in Wireshark 3.4.0 to 3.4.4 and 3.2.0 to 3.2.12 allows denial of service

## Risk And Classification

### Problem Types: CWE-770

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Zfs Storage Appliance Kit</a>	8.8	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All

## References

Reference	Source	Link
Wireshark · wnpa-sec-2021-04 · MS-WSP dissector excessive memory consumption.	MISC	<a href="#">www.wire</a>
Buildbot crash output: fuzz-2021-04-03-1597129.pcap (#17331) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	<a href="#">gitlab.com</a>
[SECURITY] Fedora 34 Update: wireshark-3.4.5-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedor</a>
[SECURITY] Fedora 33 Update: wireshark-3.4.5-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedor</a>
Debian -- Security Information -- DSA-5019-1 wireshark	DEBIAN	<a href="#">www.deb</a>
Oracle Critical Patch Update Advisory - October 2021	MISC	<a href="#">www.orac</a>

[SECURITY] Fedora 33 Update: wireshark-3.4.5-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedor</a>
[SECURITY] Fedora 34 Update: wireshark-3.4.5-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedor</a>
2021/CVE-2021-22207.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="#">gitlab.com</a>
Wireshark: Multiple vulnerabilities (GLSA 202107-21) — Gentoo security	GENTOO	<a href="#">security.g</a>
[SECURITY] [DLA 2849-1] wireshark security update	MLIST	<a href="#">lists.debian</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">178933</a> Debian Security Update for wireshark (DSA 5019-1)
<a href="#">178957</a> Debian Security Update for wireshark (DLA 2849-1)
<a href="#">179518</a> Debian Security Update for wireshark (CVE-2021-22207)
<a href="#">281491</a> Fedora Security Update for wireshark (FEDORA-2021-67691ad99d)
<a href="#">281492</a> Fedora Security Update for wireshark (FEDORA-2021-6e0508d69d)
<a href="#">296068</a> Oracle Solaris 11.4 Support Repository Update (SRU) 34.94.4 Missing (CPUAPR2021)
<a href="#">375489</a> Wireshark Protocol Memory Consumption Vulnerability (wnpa-sec-2021-04)
<a href="#">501720</a> Alpine Linux Security Update for wireshark
<a href="#">710055</a> Gentoo Linux Wireshark Multiple vulnerabilities (GLSA 202107-21)
<a href="#">750694</a> SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2021:2125-1)
<a href="#">750715</a> OpenSUSE Security Update for wireshark, libvirt, sbc, libqt5-qtmultimedia (openSUSE-SU-2021:0909-1)
<a href="#">750814</a> OpenSUSE Security Update for wireshark (openSUSE-SU-2021:2125-1)
<a href="#">901485</a> Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (7405)
<a href="#">902262</a> Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (7405-1)

© [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](#)