



# CVE-2021-39920

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

## Summary

<b>CVE</b>	CVE-2021-39920
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-11-18 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:37:00 UTC
<b>Description</b>	NULL pointer exception in the IPPUSB dissector in Wireshark 3.4.0 to 3.4.9 allows denial of service via packet injection or c

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 34 Update: wireshark-3.6.0-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorapr</a>
Fuzz job crash output: fuzz-2021-11-01-6716.pcap (#17705) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	<a href="#">gitlab.com</a>
Debian -- Security Information -- DSA-5019-1 wireshark	DEBIAN	<a href="#">www.debian.</a>
2021/CVE-2021-39920.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="#">gitlab.com</a>
[SECURITY] Fedora 34 Update: wireshark-3.6.0-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedorapr</a>
Wireshark: Multiple Vulnerabilities (GLSA 202210-04) — Gentoo security	GENTOO	<a href="#">security.gent</a>
Wireshark · wnpa-sec-2021-15 · IPPUSB dissector crash	MISC	<a href="#">www.wiresha</a>
[SECURITY] Fedora 35 Update: wireshark-3.6.0-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorapr</a>
[SECURITY] Fedora 35 Update: wireshark-3.6.0-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedorapr</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

## Vendor Comments And Credit

Discovery Credit

**LEGACY: TODO**

## Legacy QID Mappings

178933	Debian Security Update for wireshark (DSA 5019-1)
182433	Debian Security Update for wireshark (CVE-2021-39920)
282092	Fedora Security Update for wireshark (FEDORA-2021-97bd631e0a)
282134	Fedora Security Update for wireshark (FEDORA-2021-3747cf6107)
354338	Amazon Linux Security Advisory for wireshark : ALAS2022-2022-079
354457	Amazon Linux Security Advisory for wireshark : ALAS2022-2022-226
354540	Amazon Linux Security Advisory for wireshark : ALAS-2022-226
355161	Amazon Linux Security Advisory for wireshark : ALAS2023-2023-038
376095	Wireshark IPPUSB dissector Denial of Service (DoS) (wnpa-sec-2021-15)
502201	Alpine Linux Security Update for wireshark
502401	Alpine Linux Security Update for wireshark
710636	Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 202210-04)
751469	OpenSUSE Security Update for wireshark (openSUSE-SU-2021:3938-1)
751516	OpenSUSE Security Update for wireshark (openSUSE-SU-2021:1566-1)
901796	Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (7408)
902336	Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (7408-1)

© 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](#)**