



# CVE-2021-4190

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

## Summary

<b>CVE</b>	CVE-2021-4190
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-12-30 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:40:00 UTC
<b>Description</b>	Large loop in the Kafka dissector in Wireshark 3.6.0 allows denial of service via packet injection or crafted capture file

## Risk And Classification

**Problem Types:** CWE-834

## 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
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	3.6.0	All	All	All

## References

### Reference

[SECURITY] Fedora 34 Update: wireshark-3.6.1-1.fc34 - package-announce - Fedora Mailing-Lists
2021/CVE-2021-4190.json · master · GitLab.org / cves · GitLab
[SECURITY] Fedora 34 Update: wireshark-3.6.1-1.fc34 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 35 Update: wireshark-3.6.1-1.fc35 - package-announce - Fedora Mailing-Lists
Wireshark: Multiple Vulnerabilities (GLSA 202210-04) — Gentoo security
Wireshark · wnpa-sec-2021-22 · Kafka dissector infinite loop.
KAFKA dissector excessive memory and CPU consumption - denial of service (#17811) · Issues · Wireshark Foundation / wireshark · GitLab
[SECURITY] Fedora 35 Update: wireshark-3.6.1-1.fc35 - package-announce - Fedora Mailing-Lists
CVE Program record
NVD vulnerability detail

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Sharon Brizinov

## Legacy QID Mappings

183844	Debian Security Update for wireshark (CVE-2021-4190)
282259	Fedora Security Update for wireshark (FEDORA-2022-1daf93c51d)
282264	Fedora Security Update for wireshark (FEDORA-2022-30411cb3c4)
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
710636	Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 202210-04)
751705	SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2022:0375-1)
751708	OpenSUSE Security Update for wireshark (openSUSE-SU-2022:0375-1)
901853	Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (9100)
902327	Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (9100-1)

© [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](#)