



# CVE-2021-4186

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

## Summary

<b>CVE</b>	CVE-2021-4186
<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>	Crash in the Gryphon dissector in Wireshark 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture fi

## 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 35 Update: vim-8.2.4006-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: wireshark-3.6.1-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
Wireshark · wnpa-sec-2021-16 · Gryphon dissector crash	MISC	<a href="#">www.wireshark.org</a>
[SECURITY] Fedora 34 Update: wireshark-3.6.1-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 35 Update: wireshark-3.6.1-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: vim-8.2.4068-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
2021/CVE-2021-4186.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="#">gitlab.com</a>
[SECURITY] Fedora 34 Update: vim-8.2.4068-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
Wireshark: Multiple Vulnerabilities (GLSA 202210-04) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
Fuzz job crash output: fuzz-2021-11-18-10827.pcap (#17737) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	<a href="#">gitlab.com</a>
[SECURITY] Fedora 35 Update: wireshark-3.6.1-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>

CVE Program record

CVE.ORG

[www.cve.org](https://www.cve.org)

NVD vulnerability detail

NVD

[nvd.nist.gov](https://nvd.nist.gov)

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[182949](#) Debian Security Update for wireshark (CVE-2021-4186)

[282219](#) Fedora Security Update for vim (FEDORA-2022-a3d70b50f0)

[282259](#) Fedora Security Update for wireshark (FEDORA-2022-1daf93c51d)

[282264](#) Fedora Security Update for wireshark (FEDORA-2022-30411cb3c4)

[282279](#) Fedora Security Update for vim (FEDORA-2022-48b86d586f)

[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

[376218](#) Wireshark Gryphon Dissector Crash Vulnerability (wnpa-sec-2021-16)

[502201](#) Alpine Linux Security Update for wireshark

[502401](#) Alpine Linux Security Update for wireshark

[710636](#) Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 202210-04)

[752600](#) SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2022:3309-1)

[900990](#) Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (7421)

[902341](#) Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (7421-1)

© [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.cve.org). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)