



# CVE-2023-1994

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-1994
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-12 22:15:00 UTC
<b>Updated</b>	2023-11-07 04:05:00 UTC
<b>Description</b>	GQUIC dissector crash in Wireshark 4.0.0 to 4.0.4 and 3.6.0 to 3.6.12 allows denial of service via packet injection or crafted

## Risk And Classification

**Problem Types:** CWE-400

## 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>	12.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 37 Update: wireshark-4.0.5-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorapr</a>
[SECURITY] Fedora 36 Update: wireshark-3.6.13-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorapr</a>
Debian -- Security Information -- DSA-5429-1 wireshark	DEBIAN	<a href="#">www.debian.</a>
2023/CVE-2023-1994.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="#">gitlab.com</a>
Wireshark · wnpa-sec-2023-11 GQUIC dissector crash	MISC	<a href="#">www.wiresha</a>
Wireshark: Multiple Vulnerabilities (GLSA 202309-02) — Gentoo security	GENTOO	<a href="#">security.gent</a>
[SECURITY] Fedora 38 Update: wireshark-4.0.5-1.fc38 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedorapr</a>
[SECURITY] Fedora 38 Update: wireshark-4.0.5-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorapr</a>

[SECURITY] [DLA 3402-1] wireshark security update	MLIST	<a href="https://lists.debian.org">lists.debian.o</a>
[SECURITY] Fedora 37 Update: wireshark-4.0.5-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedorapr</a>
[SECURITY] Fedora 36 Update: wireshark-3.6.13-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedorapr</a>
Fuzz job crash output: fuzz-2023-03-31-6903.pcap (#18947) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	<a href="https://gitlab.com">gitlab.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">181754</a> Debian Security Update for wireshark (DLA 3402-1)
<a href="#">181872</a> Debian Security Update for wireshark (DSA 5429-1)
<a href="#">283925</a> Fedora Security Update for wireshark (FEDORA-2023-203eff67e0)
<a href="#">283926</a> Fedora Security Update for wireshark (FEDORA-2023-7af3ad9ffe)
<a href="#">284180</a> Fedora Security Update for wireshark (FEDORA-2023-f70fbf64cb)
<a href="#">355407</a> Amazon Linux Security Advisory for wireshark : ALAS2023-2023-199
<a href="#">378402</a> Wireshark GQUIC dissector crash Vulnerability (wnpa-sec-2023-11)
<a href="#">710745</a> Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 202309-02)
<a href="#">753931</a> SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2023:1931-1)

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

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