



CVE-2022-3725

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

Summary

CVE	CVE-2022-3725
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-27 17:15:00 UTC
Updated	2023-11-07 03:51:00 UTC
Description	Crash in the OPUS protocol dissector in Wireshark 3.6.0 to 3.6.8 allows denial of service via packet injection or crafted capi

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source
[SECURITY] Fedora 37 Update: wireshark-4.0.1-1.fc37 - package-announce - Fedora Mailing-Lists	
2022/CVE-2022-3725.json · master · GitLab.org / cves · GitLab	CONFIRM
Wireshark · wnpa-sec-2022-07 · OPUS dissector crash	MISC
[SECURITY] Fedora 37 Update: wireshark-4.0.1-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA
Wireshark: Multiple Vulnerabilities (GLSA 202309-02) — Gentoo security	GENTOO
Stack Overflow Write - OPUS dissector - dissect_opus() frames (#18378) · Issues · Wireshark Foundation / wireshark · GitLab	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Qiuhao Li of Zoom Video Communications, Inc.

Legacy QID Mappings

[182813](#) Debian Security Update for wireshark (CVE-2022-3725)

[283398](#) Fedora Security Update for wireshark (FEDORA-2022-cf9ae8e4ff)

[354701](#) Amazon Linux Security Advisory for wireshark : ALAS2022-2023-268

[355161](#) Amazon Linux Security Advisory for wireshark : ALAS2023-2023-038

[710745](#) Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 202309-02)

[753002](#) SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2022:4453-1)

© [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](#)