



CVE-2022-4344

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-4344
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-12 00:15:00 UTC
Updated	2023-11-07 03:57:00 UTC
Description	Memory exhaustion in the Kafka protocol dissector in Wireshark 4.0.0 to 4.0.1 and 3.6.0 to 3.6.9 allows denial of service via

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Link	T
2022/CVE-2022-4344.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.com	
[SECURITY] Fedora 36 Update: wireshark-3.6.11-1.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 37 Update: wireshark-4.0.3-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Wireshark · wnpa-sec-2022-10 · Kafka dissector memory exhaustion.	MISC	www.wireshark.org	
[SECURITY] Fedora 37 Update: wireshark-4.0.3-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 36 Update: wireshark-3.6.11-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	cc
NVD vulnerability detail	NVD	nvd.nist.gov	cc

Vendor Comments And Credit

Discovery Credit

LEGACY: Sharon Brizinov

Legacy QID Mappings

[182643](#) Debian Security Update for wireshark (CVE-2022-4344)

[283695](#) Fedora Security Update for wireshark (FEDORA-2023-9ddb9b9757)

[283697](#) Fedora Security Update for wireshark (FEDORA-2023-f9e2ad8b73)

[355179](#) Amazon Linux Security Advisory for wireshark : ALAS2023-2023-120

[355407](#) Amazon Linux Security Advisory for wireshark : ALAS2023-2023-199

[905252](#) Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (12994)

[907353](#) Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (12994-1)

© [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](#)