



CVE-2023-2857

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

Summary

CVE	CVE-2023-2857
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-26 21:15:00 UTC
Updated	2023-10-20 17:53:00 UTC
Description	BLF file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	12.0	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Link
Wireshark • wnpa-sec-2023-13 BLF file parser crash	MISC	www.wireshark.
Debian -- Security Information -- DSA-5429-1 wireshark	DEBIAN	www.debian.org
Heap buffer overflow vulnerability in BLF reader (#19063) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	gitlab.com
Wireshark: Multiple Vulnerabilities (GLSA 202309-02) — Gentoo security	GENTOO	security.gentoo.
2023/CVE-2023-2857.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Huascar Tejada

Legacy QID Mappings

[181872](#) Debian Security Update for wireshark (DSA 5429-1)

[355402](#) Amazon Linux Security Advisory for wireshark : ALAS2023-2023-197

[378527](#) Wireshark BLF file parser crash Vulnerability (wnpa-sec-2023-13)

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

[754056](#) SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2023:2320-1)

[754263](#) SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2023:3252-1)

© [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](#)