



# CVE-2023-2854

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

## Summary

<b>CVE</b>	CVE-2023-2854
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-26 21:15:00 UTC
<b>Updated</b>	2023-10-20 18:07:00 UTC
<b>Description</b>	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	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	12.0	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All

## References

Reference	Source	Link
Debian -- Security Information -- DSA-5429-1 wireshark	DEBIAN	<a href="#">www.c...</a>
Wireshark • wnpa-sec-2023-17 BLF file parser crash	MISC	<a href="#">www.v...</a>
2023/CVE-2023-2854.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="#">gitlab.</a>
Wireshark: Multiple Vulnerabilities (GLSA 202309-02) — Gentoo security	GENTOO	<a href="#">securi...</a>
Heap Buffer Overflow blf_read_apptextmessage Function (#19084) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	<a href="#">gitlab.</a>
CVE Program record	CVE.ORG	<a href="#">www.c...</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni...</a>

## 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

[378523](#) Wireshark BLF file parser crash Vulnerability (wnpa-sec-2023-17)

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

© [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](#)