



# CVE-2023-2856

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

## Summary

<b>CVE</b>	CVE-2023-2856
<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 17:53:00 UTC
<b>Description</b>	VMS TCPIPtrace 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

## 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>	10.0	All	All	All
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
Stack Buffer Overflow in parse_vms_packet Function (#19083) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	<a href="#">gitlab.com</a>
Debian -- Security Information -- DSA-5429-1 wireshark	DEBIAN	<a href="#">www.debian.org</a>
Wireshark • wnpa-sec-2023-16 VMS TCPIPtrace file parser crash	MISC	<a href="#">www.wireshark.org</a>
Wireshark: Multiple Vulnerabilities (GLSA 202309-02) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
2023/CVE-2023-2856.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="#">gitlab.com</a>
[SECURITY] [DLA 3443-1] wireshark security update	MLIST	<a href="#">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

## Vendor Comments And Credit

Discovery Credit

## LEGACY: Huascar Tejada

### Legacy QID Mappings

161124 Oracle Enterprise Linux Security Update for wireshark (ELSA-2023-6469)

161162 Oracle Enterprise Linux Security Update for wireshark (ELSA-2023-7015)

181823 Debian Security Update for wireshark (DLA 3443-1)

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

242380 Red Hat Update for wireshark (RHSA-2023:6469)

242421 Red Hat Update for wireshark (RHSA-2023:7015)

355402 Amazon Linux Security Advisory for wireshark : ALAS2023-2023-197

355792 Amazon Linux Security Advisory for wireshark : ALAS2-2023-2187

378521 Wireshark VMS TCPIPtrace file parser crash Vulnerability (wnpa-sec-2023-16)

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)

941355 AlmaLinux Security Update for wireshark (ALSA-2023:6469)

941425 AlmaLinux Security Update for wireshark (ALSA-2023:7015)

© [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](#)**