



CVE-2023-1161

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

Summary

CVE	CVE-2023-1161
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-06 21:15:00 UTC
Updated	2023-10-20 18:23:00 UTC
Description	ISO 15765 and ISO 10681 dissector crash in Wireshark 4.0.0 to 4.0.3 and 3.6.0 to 3.6.11 allows denial of service via packe

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	12.0	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference

- [Debian -- Security Information -- DSA-5429-1 wireshark](#)
- [ISO15765 and ISO10681 dissectors corrupt memory and Wireshark may crash \(#18839\) · Issues · Wireshark Foundation / wireshark · GitLab](#)
- [Wireshark: Multiple Vulnerabilities \(GLSA 202309-02\) — Gentoo security](#)
- [Wireshark · wnpa-sec-2023-08 ISO 15765 and ISO 10681 dissector crash](#)
- [\[SECURITY\] \[DLA 3402-1\] wireshark security update](#)
- [2023/CVE-2023-1161.json · master · GitLab.org / cves · GitLab](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181754 Debian Security Update for wireshark (DLA 3402-1)

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

296099 Oracle Solaris 11.4 Support Repository Update (SRU) 57.144.3 Missing (CPUAPR2023)

355175 Amazon Linux Security Advisory for wireshark : ALAS2023-2023-152

503278 Alpine Linux Security Update for wireshark

506274 Alpine Linux Security Update for wireshark

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

753888 SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2023:1762-1)

© [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](#)