CVE-2021-4183

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-4183
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-30 22:15:00 UTC
Updated	2023-11-07 03:40:00 UTC
Description	Crash in the pcapng file parser in Wireshark 3.6.0 allows denial of service via crafted capture file

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Oracle	Http Server	12.2.1.3.0	All	All	All
Application	Oracle	Http Server	12.2.1.4.0	All	All	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	All	All	All
Application	Wireshark	Wireshark	3.6.0	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 34 Update: wireshark-3.6.1-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproj
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.co
2021/CVE-2021-4183.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.com
[SECURITY] Fedora 34 Update: wireshark-3.6.1-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproj
[SECURITY] Fedora 35 Update: wireshark-3.6.1-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproj
Wireshark: Multiple Vulnerabilities (GLSA 202210-04) — Gentoo security	GENTOO	security.gentoo
heap-buffer-overflow in pcapng_process_options (#17755) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	gitlab.com
[SECURITY] Fedora 35 Update: wireshark-3.6.1-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproj
Wireshark - wnpa-sec-2021-19 - pcapng file parser crash	MISC	www.wiresharl

Wireshark · wnpa-sec-2021-19 · pcapng file parser crash	MISC	www.wireshark
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Shaohua Li

Legacy QID Mappings

- 182063 Debian Security Update for wireshark (CVE-2021-4183)
- 282259 Fedora Security Update for wireshark (FEDORA-2022-1daf93c51d)
- 282264 Fedora Security Update for wireshark (FEDORA-2022-30411cb3c4)
- 296062 Oracle Solaris 11.4 Support Repository Update (SRU) 43.113.3 Missing (CPUJAN2022)
- 376215 Wireshark Pcapng File Parser Crash Vulnerability (wnpa-sec-2021-19)
- 710636 Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 202210-04)
- 751705 SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2022:0375-1)
- 751708 OpenSUSE Security Update for wireshark (openSUSE-SU-2022:0375-1)

© 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 registred 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