CVE-2022-0583

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-0583
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-14 22:15:00 UTC
Updated	2023-11-07 03:41:00 UTC
Description	Crash in the PVFS protocol dissector in Wireshark 3.6.0 to 3.6.1 and 3.4.0 to 3.4.11 allows denial of service via packet injec

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	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference
[SECURITY] Fedora 34 Update: wireshark-3.6.2-1.fc34 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 35 Update: wireshark-3.6.2-1.fc35 - package-announce - Fedora Mailing-Lists
Wireshark · wnpa-sec-2022-03 · PVFS dissector crash
2022/CVE-2022-0583.json · master · GitLab.org / cves · GitLab
[SECURITY] Fedora 34 Update: wireshark-3.6.2-1.fc34 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 35 Update: wireshark-3.6.2-1.fc35 - package-announce - Fedora Mailing-Lists
[SECURITY] [DLA 2967-1] wireshark security update
Wireshark: Multiple Vulnerabilities (GLSA 202210-04) — Gentoo security
Heap overflow - OOB Read in PVFS2 dissector - dissect_pvfs2_getconfig_response (#17840) · Issues · Wireshark Foundation / wireshark · Gi
CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Sharon Brizinov

Legacy QID Mappings

179167 Debian Security Update for wireshark (DLA 2967-1)

181025 Debian Security Update for wireshark (CVE-2022-0583)

282433 Fedora Security Update for wireshark (FEDORA-2022-e29665a42b)

282434 Fedora Security Update for wireshark (FEDORA-2022-5a3603afe0)

296062 Oracle Solaris 11.4 Support Repository Update (SRU) 43.113.3 Missing (CPUJAN2022)

354338 Amazon Linux Security Advisory for wireshark : ALAS2022-2022-079

354457 Amazon Linux Security Advisory for wireshark : ALAS2022-2022-226

354540 Amazon Linux Security Advisory for wireshark : ALAS-2022-226

355161 Amazon Linux Security Advisory for wireshark : ALAS2023-2023-038

502201 Alpine Linux Security Update for wireshark

502402 Alpine Linux Security Update for wireshark

505569 Alpine Linux Security Update for wireshark

710636 Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 202210-04)

751796 SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2022:0722-1)

751821 OpenSUSE Security Update for wireshark (openSUSE-SU-2022:0722-1)

901033 Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (8613)

902282 Common Base Linux Mariner (CBL-Mariner) Security Update for wireshark (8613-1)

© 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