CVE-2021-22191

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-22191
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-15 18:15:00 UTC
Updated	2022-05-27 18:45:00 UTC
Description	Improper URL handling in Wireshark 3.4.0 to 3.4.3 and 3.2.0 to 3.2.11 could allow remote code execution via via packet inje

Risk And Classification

Problem Types: CWE-74

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	Oracle	Zfs Storage Appliance	8.8	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source
Code execution in Wireshark via non-http(s) schemes in URL fields (#17232) · Issues · Wireshark Foundation / wireshark · GitLab	MISC
[SECURITY] [DLA 2967-1] wireshark security update	MLIST
Wireshark · wnpa-sec-2021-03 · Wireshark could open unsafe URLs.	MISC
Wireshark: Multiple vulnerabilities (GLSA 202107-21) — Gentoo security	GENTOC
2021/CVE-2021-22191.json · master · GitLab.org / cves · GitLab	CONFIRM
Oracle Critical Patch Update Advisory - April 2021	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Lukas Euler

Legacy QID Mappings

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

180438 Debian Security Update for wireshark (CVE-2021-22191)

501719 Alpine Linux Security Update for wireshark

505572 Alpine Linux Security Update for wireshark

710055 Gentoo Linux Wireshark Multiple vulnerabilities (GLSA 202107-21)

750694 SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2021:2125-1)

750715 OpenSUSE Security Update for wireshark, libvirt, sbc, libqt5-qtmultimedia (openSUSE-SU-2021:0909-1)

750814 OpenSUSE Security Update for wireshark (openSUSE-SU-2021:2125-1)