



CVE-2020-26575

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

Summary

CVE	CVE-2020-26575
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-06 15:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	In Wireshark through 3.2.7, the Facebook Zero Protocol (aka FBZERO) dissector could enter an infinite loop. This was add

Risk And Classification

Problem Types: CWE-835

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	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Hardware	Oracle	Zfs Storage Appliance	-	All	All	All
Hardware	Oracle	Zfs Storage Appliance	-	All	All	All
Operating System	Oracle	Zfs Storage Appliance Firmware	8.8	All	All	All
Operating System	Oracle	Zfs Storage Appliance Firmware	8.8	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 32 Update: wireshark-3.4.0-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
FBZERO: Make sure our offset advances. (l471) · Merge Requests · Wireshark Foundation / wireshark · GitLab	MISC	gitlab.com
FBZERO: Make sure our offset advances. (3ff94065) · Commits · Wireshark Foundation / wireshark · GitLab	MISC	gitlab.com

[SECURITY] Fedora 32 Update: wireshark-3.4.0-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
FBZERO: Make sure our offset advances. (l472) · Merge Requests · Wireshark Foundation / wireshark · GitLab	MISC	gitlab.com
Infinite memory allocation while parsing this tcp packet. (#16887) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	gitlab.com
FBZERO: Make sure our offset advances. (l467) · Merge Requests · Wireshark Foundation / wireshark · GitLab	MISC	gitlab.com
Wireshark · wnpa-sec-2020-14 · FBZERO dissector crash	CONFIRM	www.wireshark.org
FBZERO: Make sure our offset advances. (l473) · Merge Requests · Wireshark Foundation / wireshark · GitLab	MISC	gitlab.com
[SECURITY] [DLA 2547-1] wireshark security update	MLIST	lists.debian.org
[SECURITY] Fedora 33 Update: wireshark-3.4.0-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 33 Update: wireshark-3.4.0-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Wireshark: Multiple vulnerabilities (GLSA 202011-08) — Gentoo security	GENTOO	security.gentoo.org
Oracle Critical Patch Update Advisory - January 2021	MISC	www.oracle.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [178650](#) Debian Security Update for wireshark (DLA 2547-1)
- [296070](#) Oracle Solaris 11.4 Support Repository Update (SRU) 28.82.3 Missing (CPUOCT2020)
- [501329](#) Alpine Linux Security Update for wireshark
- [501715](#) Alpine Linux Security Update for wireshark
- [750535](#) OpenSUSE Security Update for wireshark (openSUSE-SU-2020:2107-1)
- [750543](#) OpenSUSE Security Update for wireshark (openSUSE-SU-2020:2076-1)

© [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](#)