



CVE-2020-11647

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

Summary

CVE	CVE-2020-11647
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-10 21:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	In Wireshark 3.2.0 to 3.2.2, 3.0.0 to 3.0.9, and 2.6.0 to 2.6.15, the BACapp dissector could crash. This was addressed in ep

Risk And Classification

Problem Types: CWE-674

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	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:1188-1: moderate: Security update f	SUSE	lists.opensuse.org	Mailing List, Patch, Third Party
[security-announce] openSUSE-SU-2020:1199-1: moderate: Security update f	SUSE	lists.opensuse.org	Mailing List, Patch, Third Party
Wireshark: Multiple vulnerabilities (GLSA 202007-13) — Gentoo security	GENTOO	security.gentoo.org	Third Party Advisory
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org	
code.wireshark Code Review - wireshark.git/commit	MISC	code.wireshark.org	Vendor Advisory

[SECURITY] [DLA 2547-1] wireshark security update	MLIST	lists.debian.org	Mailing List, Third Party A
16474 – [oss-fuzz] #21541: Stack-overflow in fAbstractSyntaxNTType	MISC	bugs.wireshark.org	Issue Tracking, Vendor Ac
Wireshark · wnpa-sec-2020-07 · BACapp dissector crash	MISC	www.wireshark.org	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178650](#) Debian Security Update for wireshark (DLA 2547-1)

[296074](#) Oracle Solaris 11.4 Support Repository Update (SRU) 22.69.4 Missing (CPUAPR2020)

[501324](#) Alpine Linux Security Update for wireshark

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report