



CVE-2018-19857

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-19857
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-05 11:29:00 UTC
Updated	2023-11-07 02:55:00 UTC
Description	The CAF demuxer in modules/demux/caf.c in VideoLAN VLC media player 3.0.4 may read memory from an uninitialized po

Risk And Classification

Problem Types: CWE-824

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
Application	Videolan	Vlc Media Player	3.0.4	All	All	All
Application	Videolan	Vlc Media Player	3.0.4	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2019:2015-1: important: Security update	SUSE	lists.opensuse.org	
CVE-2018-19857: vlc: uninitialized memory read in caf demuxer Hans Jerry Illikainen	MISC	dyntopia.com	Exploit, Third
git.videolan.org Git - vlc.git/commit		git.videolan.org	
git.videolan.org Git - vlc.git/commit	MISC	git.videolan.org	Patch, Third I
USN-4074-1: VLC vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
[security-announce] openSUSE-SU-2019:1840-1: important: Security update	SUSE	lists.opensuse.org	
Debian -- Security Information -- DSA-4366-1 vlc	DEBIAN	www.debian.org	Third Party A
[security-announce] openSUSE-SU-2019:1897-1: important: Security update	SUSE	lists.opensuse.org	
VideoLAN VLC CVE-2018-19857 Integer Underflow Vulnerability	BID	www.securityfocus.com	Third Party A
[security-announce] openSUSE-SU-2019:1909-1: important: Security update	SUSE	lists.opensuse.org	

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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.

Free CVE JSON API cve.report/api

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