



CVE-2019-14776

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

Summary

CVE	CVE-2019-14776
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-29 19:15:00 UTC
Updated	2020-08-18 15:05:00 UTC
Description	A heap-based buffer over-read exists in DemuxInit() in demux/asf/asf.c in VideoLAN VLC media player 3.0.7.1 via a crafted

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Videolan	Vlc Media Player	3.0.7.1	All	All	All
Application	Videolan	Vlc Media Player	3.0.7.1	All	All	All

References

Reference	Source	Link	Tags
VideoLAN Security Bulletin VLC 3.0.8 - VideoLAN	CONFIRM	www.videolan.org	Patch, Vendor Advisory
Debian -- Security Information -- DSA-4504-1 vlc	DEBIAN	www.debian.org	Third Party Advisory
VLC: Multiple vulnerabilities (GLSA 201909-02) — Gentoo security	GENTOO	security.gentoo.org	
[security-announce] openSUSE-SU-2020:0545-1: moderate: Security update f	SUSE	lists.opensuse.org	
git.videolan.org Git - vlc.git/search	CONFIRM	git.videolan.org	Patch, Third Party Adviso
Bugtraq: [SECURITY] [DSA 4504-1] vlc security update	BUGTRAQ	seclists.org	Mailing List, Third Party A
USN-4131-1: VLC vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
[security-announce] openSUSE-SU-2020:0562-1: moderate: Security update f	SUSE	lists.opensuse.org	

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

[710130](#) Gentoo Linux VLC Multiple vulnerabilities (GLSA 201909-02)

© 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