



# CVE-2019-13962

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

## Summary

<b>CVE</b>	CVE-2019-13962
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-18 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:04:00 UTC
<b>Description</b>	lavc_CopyPicture in modules/codecs/avcodec/video.c in VideoLAN VLC media player through 3.0.7 has a heap-based buffer overflow

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Opensuse</a>	<a href="#">Backports Sle</a>	15.0	-	All	All
Application	<a href="#">Opensuse</a>	<a href="#">Backports Sle</a>	15.0	sp1	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Application	<a href="#">Videolan</a>	<a href="#">Vlc Media Player</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-4504-1 vlc	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
VLC: Multiple vulnerabilities (GLSA 201909-02) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
[security-announce] openSUSE-SU-2019:2015-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
git.videolan.org Git - vlc/vlc-3.0.git/commit	MISC	<a href="http://git.videolan.org">git.videolan.org</a>	Mailing List, Patch, V
[security-announce] openSUSE-SU-2020:0545-1: moderate: Security update f	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	

git.videolan.org Git - vlc/vlc-3.0.git/commit		<a href="https://git.videolan.org">git.videolan.org</a>	
[security-announce] openSUSE-SU-2019:1840-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
Bugtraq: [SECURITY] [DSA 4504-1] vlc security update	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>	
USN-4131-1: VLC vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
VideoLAN VLC CVE-2019-13962 Heap Based Buffer Overflow Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory,
[security-announce] openSUSE-SU-2019:1897-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
#22240 (avcodec picture copy heap-buffer-overflow) – VLC	MISC	<a href="https://trac.videolan.org">trac.videolan.org</a>	Exploit, Vendor Advis
[security-announce] openSUSE-SU-2020:0562-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
[security-announce] openSUSE-SU-2019:1909-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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](https://status.cve.report)