



# CVE-2018-11516

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

## Summary

<b>CVE</b>	CVE-2018-11516
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-05-28 16:29:00 UTC
<b>Updated</b>	2023-03-03 21:00:00 UTC
<b>Description</b>	The vlc_demux_chained_Delete function in input/demux_chained.c in VideoLAN VLC media player 3.0.1 allows remote att

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Videolan	Vlc Media Player	3.0.0	All	All	All
Application	Videolan	Vlc Media Player	3.0.1	All	All	All
Application	Videolan	Vlc Media Player	3.0.1	All	All	All

## References

Reference	Source
VideoLAN VLC 'input/demux_chained.c' Denial of Service Vulnerability	BID
VLC Media Player Use-After-Free Memory Error in Processing SWF Files Lets Remote Users Execute Arbitrary Code - SecurityTracker	SE
code16: Make free the VLC	MIS
VideoLAN Security Advisory 1801 - VideoLAN	CC
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[375218](#) VLC Media Player Remote Code Execution Vulnerability (VideoLAN-SA-1801)

© [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](#)