CVE-2018-11516

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

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

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	So
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	CO
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)