



CVE-2007-1921

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

Summary

CVE	CVE-2007-1921
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-10 23:19:00 UTC
Updated	2018-10-16 16:41:00 UTC
Description	LIBSNDFILE.DLL, as used by AOL Nullsoft Winamp 5.33 and possibly other products, allows remote attackers to execute a

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nullsoft	Winamp	5.33	All	All	All
Application	Nullsoft	Winamp	5.33	All	All	All

References

Reference
SecurityReason - AOL Nullsoft Winamp LIBSNDFILE.DLL Remote Memory Corruption (Off By Zero)
SecurityFocus
Winamp libsndfile.dll MAT File Handling NULL Byte Overwrite - Advisories - Secunia
Winamp LibSNDFile.DLL Component Remote Code Execution Vulnerability
www.piotrbania.com/all/adv/nullsoft-winamp-lsndfile-adv.txt
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
IBM X-Force Exchange
Winamp MATLAB/ScreamTracker/Impulse Tracker File Memory Corruption Errors Let Remote Users Execute Arbitrary Code - SecurityTracker
'[Dailydave] AOL Nullsoft Winamp LIBSNDFILE.DLL Remote Memory' - MARC
34432
CVE Program record
NVD vulnerability detail

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](#)