



CVE-2011-2696

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

Summary

CVE	CVE-2011-2696
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-07-27 02:55:00 UTC
Updated	2023-02-13 01:20:00 UTC
Description	Integer overflow in libsndfile before 1.0.25 allows remote attackers to cause a denial of service (application crash) or possib

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mega-nerd	Libsndfile	0.0.28	All	All	All
Application	Mega-nerd	Libsndfile	0.0.8	All	All	All
Application	Mega-nerd	Libsndfile	1.0.0	All	All	All
Application	Mega-nerd	Libsndfile	1.0.0	rc1	All	All
Application	Mega-nerd	Libsndfile	1.0.0	rc6	All	All
Application	Mega-nerd	Libsndfile	1.0.1	All	All	All
Application	Mega-nerd	Libsndfile	1.0.10	All	All	All
Application	Mega-nerd	Libsndfile	1.0.11	All	All	All
Application	Mega-nerd	Libsndfile	1.0.12	All	All	All
Application	Mega-nerd	Libsndfile	1.0.13	All	All	All
Application	Mega-nerd	Libsndfile	1.0.14	All	All	All
Application	Mega-nerd	Libsndfile	1.0.15	All	All	All
Application	Mega-nerd	Libsndfile	1.0.16	All	All	All
Application	Mega-nerd	Libsndfile	1.0.17	All	All	All
Application	Mega-nerd	Libsndfile	1.0.18	All	All	All
Application	Mega-nerd	Libsndfile	1.0.19	All	All	All
Application	Mega-nerd	Libsndfile	1.0.2	All	All	All

Application	Mega-nerd	Libsndfile	1.0.20	All	All	All
Application	Mega-nerd	Libsndfile	1.0.21	All	All	All
Application	Mega-nerd	Libsndfile	1.0.22	All	All	All
Application	Mega-nerd	Libsndfile	1.0.23	All	All	All
Application	Mega-nerd	Libsndfile	1.0.3	All	All	All
Application	Mega-nerd	Libsndfile	1.0.4	All	All	All
Application	Mega-nerd	Libsndfile	1.0.5	All	All	All
Application	Mega-nerd	Libsndfile	1.0.6	All	All	All
Application	Mega-nerd	Libsndfile	1.0.7	All	All	All
Application	Mega-nerd	Libsndfile	1.0.8	All	All	All
Application	Mega-nerd	Libsndfile	1.0.9	All	All	All
Application	Mega-nerd	Libsndfile	0.0.28	All	All	All
Application	Mega-nerd	Libsndfile	0.0.8	All	All	All
Application	Mega-nerd	Libsndfile	1.0.0	All	All	All
Application	Mega-nerd	Libsndfile	1.0.0	rc1	All	All
Application	Mega-nerd	Libsndfile	1.0.0	rc6	All	All
Application	Mega-nerd	Libsndfile	1.0.1	All	All	All
Application	Mega-nerd	Libsndfile	1.0.10	All	All	All
Application	Mega-nerd	Libsndfile	1.0.11	All	All	All
Application	Mega-nerd	Libsndfile	1.0.12	All	All	All
Application	Mega-nerd	Libsndfile	1.0.13	All	All	All
Application	Mega-nerd	Libsndfile	1.0.14	All	All	All
Application	Mega-nerd	Libsndfile	1.0.15	All	All	All
Application	Mega-nerd	Libsndfile	1.0.16	All	All	All
Application	Mega-nerd	Libsndfile	1.0.17	All	All	All
Application	Mega-nerd	Libsndfile	1.0.18	All	All	All
Application	Mega-nerd	Libsndfile	1.0.19	All	All	All
Application	Mega-nerd	Libsndfile	1.0.2	All	All	All
Application	Mega-nerd	Libsndfile	1.0.20	All	All	All
Application	Mega-nerd	Libsndfile	1.0.21	All	All	All
Application	Mega-nerd	Libsndfile	1.0.22	All	All	All
Application	Mega-nerd	Libsndfile	1.0.23	All	All	All
Application	Mega-nerd	Libsndfile	1.0.3	All	All	All
Application	Mega-nerd	Libsndfile	1.0.4	All	All	All
Application	Mega-nerd	Libsndfile	1.0.5	All	All	All

Application	Mega-nerd	Libsndfile	1.0.6	All	All	All
Application	Mega-nerd	Libsndfile	1.0.7	All	All	All
Application	Mega-nerd	Libsndfile	1.0.8	All	All	All
Application	Mega-nerd	Libsndfile	1.0.9	All	All	All
Application	Mega-nerd	Libsndfile	All	All	All	All

References						
Reference				Source	Link	
oss-security - Re: CVE Request -- libsndfile -- Integer overflow by processing certain PAF files				MLIST	www.o	
Bug 721234 – CVE-2011-2696 libsndfile: Application crash due integer overflow by processing certain PAF audio files				CONFIRM	bugzilla	
Ubuntu update for libsndfile - Secunia.com				SECUNIA	secuni	
Malformed Request				BID	www.s	
oss-security - Re: Re: CVE Request -- libsndfile -- Integer overflow by processing certain PAF files				MLIST	www.o	
www.mega-nerd.com/libsndfile/ChangeLog				CONFIRM	www.n	
libsndfile PAF File Processing Integer Overflow Vulnerability - Secunia.com				SECUNIA	secuni	
oss-security - Re: CVE Request -- libsndfile -- Integer overflow by processing certain PAF files				MLIST	www.o	
oss-security - Re: Re: CVE Request -- libsndfile -- Integer overflow by processing certain PAF files				MLIST	www.o	
SUSE update for libsndfile - Secunia.com				SECUNIA	secuni	
CVE-2011-2696 - Red Hat Customer Portal				MISC	access	
Debian -- Security Information -- DSA-2288-1 libsndfile				DEBIAN	www.d	
[SECURITY] Fedora 15 Update: libsndfile-1.0.25-1.fc15				FEDORA	lists.fe	
Red Hat Customer Portal				MISC	access	
oss-security - Re: CVE Request -- libsndfile -- Integer overflow by processing certain PAF files				MLIST	www.o	
Security Advisory SA45351 - Red Hat update for libsndfile - Secunia				SECUNIA	secuni	
openSUSE-SU-2011:0855				SUSE	herme	
oss-security - Re: Re: CVE Request -- libsndfile -- Integer overflow by processing certain PAF files				MLIST	www.o	
Support				REDHAT	www.r	
USN-1174-1: libsndfile vulnerability Ubuntu				UBUNTU	www.u	
Security Advisory SA45388 - Debian update for libsndfile - Secunia				SECUNIA	secuni	
libsndfile PAF File Processing Integer Overflow Vulnerability - Securelist				MISC	www.s	
oss-security - Re: CVE Request -- libsndfile -- Integer overflow by processing certain PAF files				MLIST	www.o	
oss-security - CVE Request -- libsndfile -- Integer overflow by processing certain PAF files				MLIST	www.o	
375125 – (CVE-2011-2696) <media-libs/libsndfile-1.0.25: PAF File Processing Integer Overflow (CVE-2011-2696)				CONFIRM	bugs.g	
mandriva.com				MANDRIVA	www.n	
CVE Program record				CVE.ORG	www.c	
NVD vulnerability detail				NVD	nvd.nis	

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](#)