



CVE-2007-4974

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

Summary

CVE	CVE-2007-4974
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-19 17:17:00 UTC
Updated	2011-10-18 04:00:00 UTC
Description	Heap-based buffer overflow in the flac_buffer_copy function in libsndfile 1.0.17 and earlier might allow remote attackers to e

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	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	All	All	All	All

References						
Reference				Source	Link	
[security-announce] SUSE Security Summary Report SUSE-SR:2008:001				SUSE	lists.opensuse.org	
Debian -- Security Information -- DSA-1442-1 libsndfile				DEBIAN	www.debian.org	
[SECURITY] Fedora 7 Update: libsndfile-1.0.17-2.fc7				FEDORA	www.redhat.com	
Gentoo Bug 192834 - media-libs/libsndfile-1.0.17 Heap-based buffer overflow in flac.c (CVE-2007-4974)				CONFIRM	bugs.gentoo.org	
Bug 296221 – CVE-2007-4974 Heap overflow in libsndfile triggerable by seeks				CONFIRM	bugzilla.redhat.com	
libsndfile FLAC.C Buffer Overflow Vulnerability				BID	www.securityfocus.com	
Support / Security / Advisories // MDKSA-2007:191 Mandriva				MANDRIVA	www.mandriva.com	
Debian update for libsndfile - Advisories - Secunia				SECUNIA	secunia.com	
SUSE Update for Multiple Packages - Advisories - Secunia				SECUNIA	secunia.com	
Gentoo update for libsndfile - Advisories - Secunia				SECUNIA	secunia.com	
Gentoo Linux Documentation -- libsndfile: Buffer overflow				GENTOO	security.gentoo.org	
USN-525-1: libsndfile vulnerability Ubuntu				UBUNTU	www.ubuntu.com	
Mandriva update for libsndfile - Advisories - Secunia				SECUNIA	secunia.com	
Security Advisory SA26932 - Fedora update for libsndfile - Secunia				SECUNIA	secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.com	
libsndfile "flac_buffer_copy()" Buffer Overflow Vulnerability - Advisories - Secunia				SECUNIA	secunia.com	
Ubuntu update for libsndfile - Advisories - Secunia				SECUNIA	secunia.com	
CVE Program record				CVE.ORG	www.cve.org	
NVD vulnerability detail				NVD	nvd.nist.gov	

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](#)