



CVE-2008-1686

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

Summary

CVE	CVE-2008-1686
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-08 18:05:00 UTC
Updated	2018-10-11 20:36:00 UTC
Description	Array index vulnerability in Speex 1.1.12 and earlier, as used in libfishsound 0.9.0 and earlier, including Illiminable DirectSh

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xine	Xine-lib	0.9.13	All	All	All
Application	Xine	Xine-lib	0.9.8	All	All	All
Application	Xine	Xine-lib	0.99	All	All	All
Application	Xine	Xine-lib	1.0	All	All	All
Application	Xine	Xine-lib	1.0.1	All	All	All
Application	Xine	Xine-lib	1.0.2	All	All	All
Application	Xine	Xine-lib	1.0.3a	All	All	All
Application	Xine	Xine-lib	1.1.0	All	All	All
Application	Xine	Xine-lib	1.1.1	All	All	All
Application	Xine	Xine-lib	1.1.10	All	All	All
Application	Xine	Xine-lib	1.1.10.1	All	All	All
Application	Xine	Xine-lib	1.1.11	All	All	All
Application	Xine	Xine-lib	0.9.13	All	All	All
Application	Xine	Xine-lib	0.9.8	All	All	All
Application	Xine	Xine-lib	0.99	All	All	All
Application	Xine	Xine-lib	1.0	All	All	All
Application	Xine	Xine-lib	1.0.1	All	All	All

Application	Xine	Xine-lib	1.0.2	All	All	All
Application	Xine	Xine-lib	1.0.3a	All	All	All
Application	Xine	Xine-lib	1.1.0	All	All	All
Application	Xine	Xine-lib	1.1.1	All	All	All
Application	Xine	Xine-lib	1.1.10	All	All	All
Application	Xine	Xine-lib	1.1.10.1	All	All	All
Application	Xine	Xine-lib	1.1.11	All	All	All
Application	Xine	Xine-lib	All	All	All	All
Application	Xiph	Libfishsound	0.5.41	All	All	All
Application	Xiph	Libfishsound	0.5.42	All	All	All
Application	Xiph	Libfishsound	0.6.0	All	All	All
Application	Xiph	Libfishsound	0.6.1	All	All	All
Application	Xiph	Libfishsound	0.6.2	All	All	All
Application	Xiph	Libfishsound	0.6.3	All	All	All
Application	Xiph	Libfishsound	0.7.0	All	All	All
Application	Xiph	Libfishsound	0.8.0	All	All	All
Application	Xiph	Libfishsound	0.8.1	All	All	All
Application	Xiph	Libfishsound	All	All	All	All
Application	Xiph	Libfishsound	0.5.41	All	All	All
Application	Xiph	Libfishsound	0.5.42	All	All	All
Application	Xiph	Libfishsound	0.6.0	All	All	All
Application	Xiph	Libfishsound	0.6.1	All	All	All
Application	Xiph	Libfishsound	0.6.2	All	All	All
Application	Xiph	Libfishsound	0.6.3	All	All	All
Application	Xiph	Libfishsound	0.7.0	All	All	All
Application	Xiph	Libfishsound	0.8.0	All	All	All
Application	Xiph	Libfishsound	0.8.1	All	All	All
Application	Xiph	Speex	1.0.2	All	All	All
Application	Xiph	Speex	1.0.3	All	All	All
Application	Xiph	Speex	1.0.4	All	All	All
Application	Xiph	Speex	1.0.5	All	All	All
Application	Xiph	Speex	1.1.1	All	All	All
Application	Xiph	Speex	1.1.10	All	All	All
Application	Xiph	Speex	1.1.11	All	All	All
Application	Xiph	Speex	1.1.11.1	All	All	All

Application	Xiph	Speex	1.1.2	All	All	All
Application	Xiph	Speex	1.1.3	All	All	All
Application	Xiph	Speex	1.1.4	All	All	All
Application	Xiph	Speex	1.1.5	All	All	All
Application	Xiph	Speex	1.1.6	All	All	All
Application	Xiph	Speex	1.1.7	All	All	All
Application	Xiph	Speex	1.1.8	All	All	All
Application	Xiph	Speex	1.1.9	All	All	All
Application	Xiph	Speex	1.0.2	All	All	All
Application	Xiph	Speex	1.0.3	All	All	All
Application	Xiph	Speex	1.0.4	All	All	All
Application	Xiph	Speex	1.0.5	All	All	All
Application	Xiph	Speex	1.1.1	All	All	All
Application	Xiph	Speex	1.1.10	All	All	All
Application	Xiph	Speex	1.1.11	All	All	All
Application	Xiph	Speex	1.1.11.1	All	All	All
Application	Xiph	Speex	1.1.2	All	All	All
Application	Xiph	Speex	1.1.3	All	All	All
Application	Xiph	Speex	1.1.4	All	All	All
Application	Xiph	Speex	1.1.5	All	All	All
Application	Xiph	Speex	1.1.6	All	All	All
Application	Xiph	Speex	1.1.7	All	All	All
Application	Xiph	Speex	1.1.8	All	All	All
Application	Xiph	Speex	1.1.9	All	All	All
Application	Xiph	Speex	All	All	All	All

References

Reference	Source	Link
Gentoo update for speex - Advisories - Secunia	SECUNIA	secunia
USN-611-2: vorbis-tools vulnerability Ubuntu	UBUNTU	www.ubuntu.com
Webmail - OVH	VUPEN	www.ovh.com
Debian update for xine-lib - Advisories - Secunia	SECUNIA	secunia
FishSound Library Remote Speex Decoding Code Execution Vulnerability	BID	www.bidsa.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
SDL_sound Speex Header Processing Vulnerability - Advisories - Secunia	SECUNIA	secunia
xine-lib Speex Header Processing Vulnerability - Advisories - Secunia	SECUNIA	secunia

Fedora update for speex - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia
Ubuntu update for speex - Advisories - Secunia	SECUNIA	secunia
[SECURITY] Fedora 8 Update: libfishsound-0.9.1-1.fc8	FEDORA	www.re
Ubuntu update for gst-plugins-good0.10 - Advisories - Secunia	SECUNIA	secunia
USN-611-1: Speex vulnerability Ubuntu	UBUNTU	www.ub
Webmail - OVH	VUPEN	www.vu
Webmail - OVH	VUPEN	www.vu
USN-635-1: xine-lib vulnerabilities Ubuntu	UBUNTU	www.ub
Support / Security / Advisories // MDVSA-2008:094 Mandriva	MANDRIVA	www.m
oCERT.org - oCERT Advisories	MISC	www.oc
oCERT.org - oCERT Advisories	MISC	www.oc
SecurityFocus	BUGTRAQ	www.se
Debian -- Security Information -- DSA-1585-1 speex	DEBIAN	www.de
Speex Validation Flaw in Speex Decoder Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.se
Repository / Oval Repository	OVAL	oval.cis
[SECURITY] Fedora 8 Update: speex-1.2-0.4.beta2	FEDORA	www.re
About Secunia Research Flexera	SECUNIA	secunia
Sweep Speex Header Processing Vulnerability - Advisories - Secunia	SECUNIA	secunia
Webmail - OVH	VUPEN	www.vu
Speex: User-assisted execution of arbitrary code — Gentoo Linux Documentation	GENTOO	security
Ubuntu update for vorbis-tools - Advisories - Secunia	SECUNIA	secunia
Support / Security / Advisories // MDVSA-2008:124 Mandriva	MANDRIVA	www.m
blog.kfish.org: Release: libfishsound 0.9.1	CONFIRM	blog.kfi
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia
Security Announcement	SUSE	www.nc
Debian update for libfishsound - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia
[security-announce] SUSE Security Summary Report SUSE-SR:2008:012	SUSE	lists.op
Red Hat update for speex - Advisories - Secunia	SECUNIA	secunia
SourceForge.net: Files	CONFIRM	sourcef
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	slackwa
SourceForge.net: xine - a free video player: Files	CONFIRM	sourcef
Ubuntu update for xine-lib - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia
libfishsound Speex Header Processing Vulnerability - Advisories - Secunia	SECUNIA	secunia
www.metadecks.org/software/sweep/news.html	CONFIRM	www.m

[Speex-dev] libfishsound 0.9.1 Release	MLIST	lists.xipl
[SECURITY] Fedora 7 Update: speex-1.2-0.3.beta1	FEDORA	www.re
Debian update for speex - Advisories - Community	SECUNIA	secunia
Fedora update for libfishsound - Advisories - Community	SECUNIA	secunia
Debian -- Security Information -- DSA-1586-1 xine-lib	DEBIAN	www.de
Debian -- Security Information -- DSA-1584-1 libfishsound	DEBIAN	www.de
USN-611-3: GStreamer Good Plugins vulnerability Ubuntu	UBUNTU	www.ut
rhn.redhat.com Red Hat Support	REDHAT	www.re
Support / Security / Advisories // MDVSA-2008:093 Mandriva	MANDRIVA	www.m:
Support / Security / Advisories // MDVSA-2008:092 Mandriva	MANDRIVA	www.m:
VLC Media Player Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia
Webmail - OVH	VUPEN	www.vu
Webmail - OVH	VUPEN	www.vu
Webmail - OVH	VUPEN	www.vu
vorbis-tools Speex Header Processing Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)