



# CVE-2008-1423

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

## Summary

<b>CVE</b>	CVE-2008-1423
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-05-16 12:54:00 UTC
<b>Updated</b>	2017-09-29 01:30:00 UTC
<b>Description</b>	Integer overflow in a certain quantvals and quantlist calculation in Xiph.org libvorbis 1.2.0 and earlier allows remote attacker

## Risk And Classification

**Problem Types:** CWE-189

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	2.1	All	as	All
Operating System	Redhat	Enterprise Linux	2.1	All	es	All
Operating System	Redhat	Enterprise Linux	2.1	All	ws	All
Operating System	Redhat	Enterprise Linux	5	All	client	All
Operating System	Redhat	Enterprise Linux	5	All	client_workstation	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	2.1	All	as	All
Operating System	Redhat	Enterprise Linux	2.1	All	es	All
Operating System	Redhat	Enterprise Linux	2.1	All	ws	All
Operating System	Redhat	Enterprise Linux	5	All	client	All
Operating System	Redhat	Enterprise Linux	5	All	client_workstation	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium	All
Application	Xiph.org	Libvorbis	1.0.0	All	All	All
Application	Xiph.org	Libvorbis	1.0.1	All	All	All
Application	Xiph.org	Libvorbis	1.1.0	All	All	All

Application	<a href="#">Xiph.org</a>	<a href="#">Libvorbis</a>	1.1.1	All	All	All
Application	<a href="#">Xiph.org</a>	<a href="#">Libvorbis</a>	1.1.2	All	All	All
Application	<a href="#">Xiph.org</a>	<a href="#">Libvorbis</a>	1.2.0	All	All	All
Application	<a href="#">Xiph.org</a>	<a href="#">Libvorbis</a>	1.0.0	All	All	All
Application	<a href="#">Xiph.org</a>	<a href="#">Libvorbis</a>	1.0.1	All	All	All
Application	<a href="#">Xiph.org</a>	<a href="#">Libvorbis</a>	1.1.0	All	All	All
Application	<a href="#">Xiph.org</a>	<a href="#">Libvorbis</a>	1.1.1	All	All	All
Application	<a href="#">Xiph.org</a>	<a href="#">Libvorbis</a>	1.1.2	All	All	All
Application	<a href="#">Xiph.org</a>	<a href="#">Libvorbis</a>	1.2.0	All	All	All

## References

Reference	Source	Link
Support / Security / Advisories // MDVSA-2008:102   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>
Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
Fedora update for libvorbis - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
libvorbis Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
[SECURITY] Fedora 9 Update: libvorbis-1.2.0-4.fc9	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
Bug 440709 – CVE-2008-1423 vorbis: integer overflow caused by huge codebooks	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
libvorbis Bugs Let Remote Users Deny Service or Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>
USN-682-1: libvorbis vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
Ubuntu update for libvorbis - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
[SECURITY] Fedora 7 Update: libvorbis-1.1.2-4.fc7	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
[security-announce] SUSE Security Summary Report SUSE-SR:2008:012	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
[SECURITY] Fedora 8 Update: libvorbis-1.2.0-2.fc8	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
Red Hat update for libvorbis - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
libvorbis Multiple Remote Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Gentoo update for libvorbis - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Debian update for libvorbis - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Debian -- Security Information -- DSA-1591-1 libvorbis	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
libvorbis: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>
Red Hat update for libvorbis - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>

Webmail   OVH- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)