



# CVE-2009-1274

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2009-1274
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-04-08 18:30:00 UTC
<b>Updated</b>	2018-10-10 19:35:00 UTC
<b>Description</b>	Integer overflow in the qt_error parse_trak_atom function in demuxers/demux_qt.c in xine-lib 1.1.16.2 and earlier allows remote users to execute arbitrary code with root privileges. <a href="#">View details</a>

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.1.11.1	All	All	All
Application	Xine	Xine-lib	1.1.12	All	All	All
Application	Xine	Xine-lib	1.1.13	All	All	All
Application	Xine	Xine-lib	1.1.14	All	All	All
Application	Xine	Xine-lib	1.1.15	All	All	All
Application	Xine	Xine-lib	1.1.16.1	All	All	All
Application	Xine	Xine-lib	1.1.16.2	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	<a href="#">Xine</a>	<a href="#">Xine-lib</a>	1.1.11.1	All	All	All
Application	<a href="#">Xine</a>	<a href="#">Xine-lib</a>	1.1.12	All	All	All
Application	<a href="#">Xine</a>	<a href="#">Xine-lib</a>	1.1.13	All	All	All
Application	<a href="#">Xine</a>	<a href="#">Xine-lib</a>	1.1.14	All	All	All
Application	<a href="#">Xine</a>	<a href="#">Xine-lib</a>	1.1.15	All	All	All
Application	<a href="#">Xine</a>	<a href="#">Xine-lib</a>	1.1.16.1	All	All	All
Application	<a href="#">Xine</a>	<a href="#">Xine-lib</a>	1.1.16.2	All	All	All

## References

Reference	Source	L
IBM X-Force Exchange	XF	e
xine-lib Integer Overflow in Processing QuickTime Media Files Lets Remote Execute Arbitrary Code - SecurityTracker	SECTRACK	v
Support / Security / Advisories // MDVSA-2009:298   Mandriva	MANDRIVA	v
Support / Security / Advisories // MDVSA-2009:299   Mandriva	MANDRIVA	v
53288	OSVDB	c
xine-lib STTS QuickTime Atom Remote Buffer Overflow Vulnerability	BID	v
SecurityFocus	BUGTRAQ	v
SUSE Update for Multiple Packages - Advisories - Community	SECUNIA	s
[SECURITY] Fedora 9 Update: xine-lib-1.1.16.3-1.fc9	FEDORA	v
bugs.xine-project.org/show_bug.cgi	CONFIRM	t
SourceForge.net: xine - a free video player: Files	CONFIRM	s
xine-lib STTS Quicktime Atom Integer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	s
Fedora update for xine-lib - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	s
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	v
www.trapkit.de/advisories/TKADV2009-005.txt	MISC	v
[SECURITY] Fedora 10 Update: xine-lib-1.1.16.3-1.fc10	FEDORA	v
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:011	SUSE	li
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

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

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](#)**