



# CVE-2008-1767

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

## Summary

<b>CVE</b>	CVE-2008-1767
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-05-23 15:32:00 UTC
<b>Updated</b>	2017-09-29 01:30:00 UTC
<b>Description</b>	Buffer overflow in pattern.c in libxslt before 1.1.24 allows context-dependent attackers to cause a denial of service (crash) a

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Desktop	3	All	All	All
Operating System	Redhat	Desktop	3	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	3.0	All	as	All
Operating System	Redhat	Enterprise Linux	3.0	All	es	All
Operating System	Redhat	Enterprise Linux	3.0	All	ws	All
Operating System	Redhat	Enterprise Linux	4.0	All	as	All
Operating System	Redhat	Enterprise Linux	4.0	All	es	All
Operating System	Redhat	Enterprise Linux	4.0	All	ws	All
Operating System	Redhat	Enterprise Linux	5.0	All	server	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	3.0	All	as	All
Operating System	Redhat	Enterprise Linux	3.0	All	es	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	ws	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	as	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	es	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	ws	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	5.0	All	server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	5	All	client	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	5	All	client	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop Workstation</a>	5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop Workstation</a>	5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	itanium	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	itanium	All

## References

Reference	Source
Apple iPhone / iPod touch Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Apple Safari Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
About the security content of Safari 3.2	CONFIRM
Bug 527297 – xsltproc crashes when applying a transform to an xml document	CONFIRM
Debian update for libxslt - Advisories - Secunia	SECUNIA
libxslt XSL File Processing Buffer Overflow Vulnerability	BID
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Repository / Oval Repository	OVAL
RETIRED: Apple Mac OS X 2008-007 Multiple Security Vulnerabilities	BID
rhn.redhat.com   Red Hat Support	REDHAT
APPLE-SA-2008-07-11 iPhone 2.0 and iPod touch 2.0	APPLE
About Security Update 2008-007	CONFIRM
IBM X-Force Exchange	XF
Security Announcement	SUSE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
SecurityTracker.com Archives - libxslt XSL Style Sheet Array Overflow May Let Remote Users Execute Arbitrary Code	SECTRACK
Ubuntu update for libxslt - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Webmail   OVH- OVH	VUPEN
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
White Paper: Security Updates for Open Enterprise 10.0	SENTINEL

libxslt: Execution of arbitrary code — Gentoo Linux Documentation	GENTOO
APPLE-SA-2008-10-09 Security Update 2008-007	APPLE
Gentoo update for libxslt - Advisories - Secunia	SECUNIA
Debian -- Security Information -- DSA-1589-1 libxslt	DEBIAN
libxslt XSL File Processing Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Support / Security / Advisories // MDVSA-2008:151   Mandriva	MANDRIVA
Red Hat update for libxslt - Advisories - Secunia	SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
APPLE-SA-2008-11-13 Safari 3.2	APPLE
USN-633-1: libxslt vulnerabilities   Ubuntu	UBUNTU
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)**