



# CVE-2004-0989

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

## Summary

<b>CVE</b>	CVE-2004-0989
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-03-01 05:00:00 UTC
<b>Updated</b>	2017-10-11 01:29:00 UTC
<b>Description</b>	Multiple buffer overflows in libXML 2.6.12 and 2.6.13 (libxml2), and possibly other versions, may allow remote attackers to e

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ia64	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ppc	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ia64	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ppc	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml</a>	1.8.17	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml</a>	1.8.17	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.5.11	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.11	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.12	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.13	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.14	All	All	All

Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.6	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.7	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.8	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.9	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.5.11	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.11	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.12	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.13	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.14	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.6	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.7	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.8	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.9	All	All	All
Application	<a href="#">Xmlstarlet</a>	<a href="#">Command Line Xml Toolkit</a>	0.9.1	All	All	All
Application	<a href="#">Xmlstarlet</a>	<a href="#">Command Line Xml Toolkit</a>	0.9.1	All	All	All

## References

### Reference

Secunia - Advisories - Libxml2 Multiple Buffer Overflows

11179

Home - Conectiva

Support

'libxml2 remote buffer overflows (not in xml parsing code though)' - MARC

Repository / Oval Repository

IBM X-Force Exchange

IBM X-Force Exchange

11180

Debian -- Security Information -- DSA-582-1 libxml

rhn.redhat.com | Red Hat Support

Repository / Oval Repository

IBM X-Force Exchange

IBM X-Force Exchange

P-029: libxml and libxml2 Buffer Overflow

SecurityTracker.com Archives - Libxml2 URL Parsing and DNS Resolution Buffer Overflows May Let Remote Users Execute Arbitrary Code

11324

Security Announcement
Libxml2 Multiple Remote Stack Buffer Overflow Vulnerabilities
Gentoo Linux Documentation -- libxml2: Remotely exploitable buffer overflow
APPLE-SA-2005-01-25 Security Update 2005-001
usn/usn-89-1 - Ubuntu Linux
CVE Program record
NVD vulnerability detail

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](#)**