



# CVE-2004-0110

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

## Summary

<b>CVE</b>	CVE-2004-0110
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-03-15 05:00:00 UTC
<b>Updated</b>	2017-10-11 01:29:00 UTC
<b>Description</b>	Buffer overflow in the (1) nanohttp or (2) nanoftp modules in XMLSoft Libxml 2 (Libxml2) 2.6.0 through 2.6.5 allow remote a

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.3	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.4	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.3	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.4	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="#">Libxml</a>	1.8.17	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.4.19	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.4.23	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.5.10	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>	2.5.4	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.0	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.1	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.2	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.3	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.4	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.5	All	All	All

Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.4.19	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.4.23	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.5.10	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>	2.5.4	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.0	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.1	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.2	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.3	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.4	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.6.5	All	All	All

## References

Reference	Source	Link	Tags
US-CERT Vulnerability Note VU#493966	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>	US Gov
libxml2 Remote URI Parsing Buffer Overrun Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Patch, V
Debian -- Security Information -- DSA-455-1 libxml	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
<a href="http://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	
Releases	CONFIRM	<a href="http://www.xmlsoft.org">www.xmlsoft.org</a>	
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>	
'TSLSA-2004-0010 - libxml2' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>	
Gentoo Linux Documentation -- Libxml2 URI Parsing Buffer Overflow Vulnerabilities	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
'[OpenPKG-SA-2004.003] OpenPKG Security Advisory (libxml)' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
<a href="http://redhat.com">redhat.com</a>   Red Hat Support	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>	Patch, V
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>	
<a href="http://redhat.com">redhat.com</a>   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>	
Secunia - Advisories - Libxml2 URI Parsing Buffer Overflow Vulnerabilities	SECUNIA	<a href="http://secunia.com">secunia.com</a>	
O-086: Red Hat Updated libxml2 Packages Fix Security Vulnerability	CIAC	<a href="http://www.ciac.org">www.ciac.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonic

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](#)**