



CVE-2016-3627

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-3627
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-17 14:08:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-deper

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Hp	Icewall Federation Agent	3.0	All	All	All
Application	Hp	Icewall Federation Agent	3.0	All	All	All
Application	Hp	Icewall File Manager	3.0	All	All	All
Application	Hp	Icewall File Manager	3.0	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

References

Reference

USN-2994-1: libxml2 vulnerabilities | Ubuntu

Document Display | HPE Support Center

Debian -- Security Information -- DSA-3593-1 libxml2

Oracle Linux Bulletin - July 2016

Full Disclosure: CVE-2016-3627 CVE-2016-3705: libxml2: stack overflow in xml validator (parser)

oss-security - Re: CVE request: Stack exhaustion in libxml2 parsing xml files in recover mode

[R7] LCE 4.8.1 Fixes Multiple Vulnerabilities - Security Advisory | Tenable™

oss-security - CVE request: Stack exhaustion in libxml2 parsing xml files in recover mode

McAfee Security Bulletin: McAfee Web Gateway update fixes several vulnerabilities related to xml parsing

Red Hat Customer Portal

Oracle VM Server for x86 Bulletin - July 2016

openSUSE-SU-2016:1298-1: moderate: Security update for libxml2

libxml2: Multiple vulnerabilities (GLSA 201701-37) — Gentoo security

Libxml2 'malloc.c' CVE-2016-3627 Denial of Service Vulnerability

openSUSE-SU-2016:1446-1: moderate: Security update for libxml2

Red Hat Customer Portal

Libxml2 Memory Allocation Error in xmlStringGetNodeList() Lets Remote Users Consume Excessive Memory Resources - SecurityTracker

Oracle Solaris Bulletin - July 2016

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](#)