



CVE-2015-7498

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

Summary

CVE	CVE-2015-7498
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-15 21:59:00 UTC
Updated	2023-02-12 23:15:00 UTC
Description	Heap-based buffer overflow in the xmlParseXmlDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent a

Risk And Classification

Problem Types: CWE-119

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	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	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	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	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	Redhat	Enterprise Linux Desktop	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-3430-1 libxml2	DEBIAN	www.deb
Bug 1281879 – CVE-2015-7498 libxml2: Heap-based buffer overflow in xmlParseXmlDecl	CONFIRM	bugzilla.r
RHSA-2015:2549	REDHAT	rhn.redha
CVE-2015-7498 - Red Hat Customer Portal	MISC	access.re
Avoid processing entities after encoding conversion failures (afd27c21) · Commits · GNOME / libxml2 · GitLab	CONFIRM	git.gnome
openSUSE-SU-2016:0106-1: moderate: Security update for libxml2	SUSE	lists.open
USN-2834-1: libxml2 vulnerabilities Ubuntu	UBUNTU	www.ubu
Red Hat Customer Portal	MISC	access.re
Red Hat Customer Portal	MISC	access.re
openSUSE-SU-2015:2372-1: moderate: Security update for libxml2	SUSE	lists.open
'[security bulletin] HPSBGN03537 rev.1 - HPE IceWall Federation Agent and IceWall File Manager runnin' - MARC	HP	marc.info
libxml2 CVE-2015-7498 Denial of Service Vulnerability	BID	www.seci
RHSA-2016:1089	REDHAT	rhn.redha
Releases	CONFIRM	xmlsoft.o
Oracle Linux Bulletin - October 2015	CONFIRM	www.orac
RHSA-2015:2550	REDHAT	rhn.redha
libxml2: Multiple vulnerabilities (GLSA 201701-37) — Gentoo security	GENTOO	security.g
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.re
Document Display HPE Support Center	CONFIRM	h20566.w
Libxml2 Multiple Flaws Let Remote Users Deny Service and Cause Other Unspecified Impacts - SecurityTracker	SECTRACK	www.seci
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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](#)