CVE-2015-8241

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-8241
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-15 21:59:00 UTC
Updated	2017-09-14 01:29:00 UTC
Description	The xmlNextChar function in libxml2 2.9.2 does not properly check the state, which allows context-dependent attackers to c

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
RHSA-2015:2549	REDHAT	rhn.redha
oss-security - Re: Buffer overflow in libxml2	MLIST	www.ope
openSUSE-SU-2016:0106-1: moderate: Security update for libxml2	SUSE	lists.open
USN-2834-1: libxml2 vulnerabilities | Ubuntu	UBUNTU	www.ubu
oss-security - Buffer overflow in libxml2	MLIST	www.ope
Avoid extra processing of MarkupDecl when EOF (ab2b9a93) · Commits · GNOME / libxml2 · GitLab	CONFIRM	git.gnome
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
RHSA-2016:1089	REDHAT	rhn.redha
Oracle Linux Bulletin - October 2015	CONFIRM	www.orac
RHSA-2015:2550	REDHAT	rhn.redha
Libxml2 'parser.c' Buffer Overflow Vulnerability	BID	www.sec
Bug 1281936 – CVE-2015-8241 libxml2: Buffer overread with XML parser in xmlNextChar	CONFIRM	bugzilla.r
Document Display | HPE Support Center	CONFIRM	h20566.w
Libxml2 Multiple Flaws Let Remote Users Deny Service and Cause Other Unspecified Impacts - SecurityTracker	SECTRACK	www.sec
Bug 756263 – Buffer overead with XML parser in xmlNextChar, causes segfault when compiled with ASAN	CONFIRM	bugzilla.g
Oracle Solaris Bulletin - January 2016	CONFIRM	www.orac
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 and Source URL Uptime Status status.cve.report