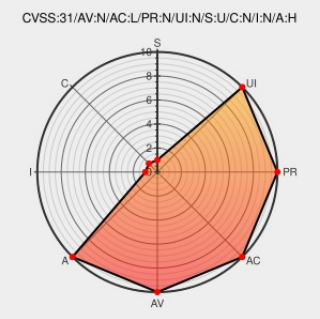
CVE-2015-8806

Published on: 04/13/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-8806

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

dict.c in libxml2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via an unexpected character immediately after the "<!DOCTYPE html" substring in a crafted HTML document.

CVE-2015-8806 has been assigned by security@debian.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
USN-2994-1: libxml2 vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2994-1
Debian -- Security Information -- DSA-3593-1 libxml2	Third Party Advisory	DEBIAN DSA-3593

	www.debian.org Depreciated Link text/html	
oss-security - Re: Out-of-bounds Read in the libxml2's htmlParseNameComplex() function	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160203 Re: Out-of-bounds Read in the libxml2's htmlParseNameComplex() function
libxml2: Multiple vulnerabilities (GLSA 201701-37) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201701-37
libxml2 CVE-2015-8806 Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 82071
Bug 749115 – Heap-buffer overread in libxml2/dict.c on fuzzed html input	Issue Tracking Vendor Advisory bugzilla.gnome.org text/html	MISC bugzilla.gnome.org/show_bug.cgi?id=749115
Oracle Solaris Bulletin - July 2016	Third Party Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinjul2016-3090568.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	Xmlsoft	Libxml2	All	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

- cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:
- cpe:2.3:a:xmlsoft:libxml2:*:*:*:*:*:*:*:*:
- cpe:2.3:a:xmlsoft:libxml2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→