



# CVE-2016-1683

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

## Summary

<b>CVE</b>	CVE-2016-1683
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-06-05 23:59:00 UTC
<b>Updated</b>	2023-11-07 02:30:00 UTC
<b>Description</b>	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles namespace nodes, which a

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise</a>	12.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise</a>	12.0	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxslt</a>	All	All	All	All

## References

### Reference

[Chromium: Multiple vulnerabilities \(GLSA 201607-07\) — Gentoo security](#)

[About the security content of iCloud for Windows 5.2.1 - Apple Support](#)

[About the security content of OS X El Capitan v10.11.6 and Security Update 2016-004 - Apple Support](#)

[APPLE-SA-2016-07-18-4 tvOS 9.2.2](#)

[APPLE-SA-2016-07-18-2 iOS 9.3.3](#)

[Apple iTunes APPLE-SA-2016-07-18-6 Multiple Memory Corruption Vulnerabilities](#)

[Chrome Releases: Stable Channel Update](#)

[About the security content of iOS 9.3.3 - Apple Support](#)

[\[SECURITY\] Fedora 30 Update: mingw-libxslt-1.1.33-1.fc30 - package-announce - Fedora Mailing-Lists](#)

[APPLE-SA-2016-07-18-1 OS X El Capitan v10.11.6 and Security Update 2016-004](#)

[APPLE-SA-2016-07-18-6 iTunes 12.4.2](#)

[1340016 – \(CVE-2016-1683\) CVE-2016-1683 chromium-browser: out-of-bounds access in libxslt](#)

[APPLE-SA-2016-07-18-3 watchOS 2.2.2](#)

[\[security-announce\] openSUSE-SU-2016:1496-1: important: Security update](#)

[About the security content of watchOS 2.2.2 - Apple Support](#)

[Google Chrome Multiple Flaws Lets Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, and Execute Arbitrary Code](#)

[\[security-announce\] openSUSE-SU-2016:1433-1: important: Security update](#)

[Google Chrome Prior to 51.0.2704.63 Multiple Security Vulnerabilities](#)

[Debian -- Security Information -- DSA-3590-1 chromium-browser](#)

[Fix xsltNumberFormatGetMultipleLevel \(d182d8f6\) · Commits · GNOME / libxslt · GitLab](#)

[About the security content of tvOS 9.2.2 - Apple Support](#)

[Debian -- Security Information -- DSA-3605-1 libxslt](#)

[\[SECURITY\] Fedora 30 Update: mingw-libxslt-1.1.33-1.fc30 - package-announce - Fedora Mailing-Lists](#)

[About the security content of iTunes 12.4.2 for Windows - Apple Support](#)

[Issue 583156 - chromium - An open-source project to help move the web forward. - Monorail](#)

[Red Hat Customer Portal](#)

[\[security-announce\] openSUSE-SU-2016:1430-1: important: Security update](#)

[CVE-2016-1683 chromium-browser: out-of-bounds access in libxslt](#)

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](#)**