



# CVE-2016-5131

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

## Summary

<b>CVE</b>	CVE-2016-5131
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-07-23 19:59:00 UTC
<b>Updated</b>	2023-11-07 02:32:00 UTC
<b>Description</b>	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attacker

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Iphone Os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Iphone Os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Tv os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Tv os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Watchos</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Watchos</a>	All	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>	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>	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>	9.0	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>	9.0	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All

Application	Google	Chrome	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	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 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
Operating System	Suse	Linux Enterprise	12.0	All	All	All
Operating System	Suse	Linux Enterprise	12.0	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

## References

### Reference

[security-announce] openSUSE-SU-2016:1869-1: important: Security update

APPLE-SA-2016-09-20-3 iOS 10

Issue 2127493002: Delete obsolete XPointer range-to function. - Code Review

Android Security Bulletin—May 2017 | Android Open Source Project

Chromium: Multiple vulnerabilities (GLSA 201610-09) — Gentoo security

About the security content of macOS Sierra 10.12 - Apple Support

About the security content of watchOS 3 - Apple Support

About the security content of tvOS 10 - Apple Support

Google Android Multiple Flaws Let Remote Users Deny Service, Obtain Potentially Sensitive Information, and Execute Arbitrary Code and Let

APPLE-SA-2016-09-20 macOS Sierra 10.12

[security-announce] openSUSE-SU-2016:1918-1: important: Security update

USN-3041-1: Oxide vulnerabilities | Ubuntu

Google Chrome Multiple Flaws Lets Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, Spoof URLs, and

Red Hat Customer Portal

[security-announce] openSUSE-SU-2016:1868-1: important: Security update

APPLE-SA-2016-09-20-5 watchOS 3

Google Chrome Multiple Flaws Lets Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, Spoof URLs, and

Google Chrome Prior to 52.0.2743.82 Multiple Security Vulnerabilities

[security-announce] openSUSE-SU-2016:1865-1: important: Security update

APPLE-SA-2016-09-20-6 tvOS 10

Debian -- Security Information -- DSA-3637-1 chromium-browser

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

623378 - chromium - An open-source project to help move the web forward. - Monorail

Bug 1358641 – CVE-2016-5131 chromium-browser: use-after-free in libxml

About the security content of iOS 10 - Apple Support

Chrome Releases: Stable Channel Update

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[377223](#) Alibaba Cloud Linux Security Update for libxml2 (ALINUX2-SA-2020:0077)

[500346](#) Alpine Linux Security Update for libxml2

[504109](#) Alpine Linux Security Update for libxml2

[591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

© [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](#)**