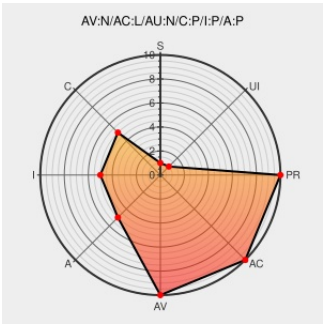
CVE-2015-1237

Published on: 04/19/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1237

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



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

Use-after-free vulnerability in the RenderFrameImpl::OnMessageReceived function in content/renderer/render_frame_impl.cc in Google Chrome before 42.0.2311.90 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger renderer IPC messages during a detach operation.

CVE-2015-1237 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3238-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3238
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Bypass Same-Origin Restrictions - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1032209
openSUSE-SU-2015:0748-1: moderate: Security update for Chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:0748
Red Hat Customer Portal	web.archive.org text/html	REDHAT RHSA-2015:0816

	Inactive Link Not Archived	
openSUSE-SU-2015:1887-1: moderate: Security update for chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1887
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2015/04/stable-channel-update_14.html
USN-2570-1: Oxide vulnerabilities | Ubuntu	ubuntu.com text/html	UBUNTU USN-2570-1
Issue 1007123003: Clear RenderFrameImpl::frame_ pointer after deleting it. - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1007123003
Chromium: Multiple vulnerabilities (GLSA 201506-04) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201506-04
Issue 461191 - chromium - Security: UNKNOWN in RenderFrameImpl::OnMessageReceived - An open-source project to help move the web forward. - Google Project Hosting	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=461191

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	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Google	Chrome	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→