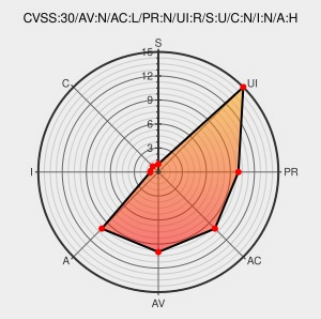
CVE-2016-1689

Published on: 06/05/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:04 PM UTC

CVE-2016-1689

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



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

Heap-based buffer overflow in content/renderer/media/canvas_capture_handler.cc in Google Chrome before 51.0.2704.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.

CVE-2016-1689 has been assigned by security@google.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Chromium: Multiple vulnerabilities (GLSA 201607-07) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201607-07
Chrome Releases: Stable Channel Update	Vendor Advisory	CONFIRM

Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2016/05/stable-channel-update_25.html
[security-announce] openSUSE-SU-2016:1496-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1496
[security-announce] openSUSE-SU-2016:1433-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1433
Google Chrome Prior to 51.0.2704.63 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 90876
Debian -- Security Information -- DSA-3590-1 chromium-browser	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3590
Issue 1918073003: Fix odd size and visible rect issues in CanvasCaptureHandler - Code Review	Issue Tracking codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1918073003
Google Chrome Multiple Flaws Lets Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, and Execute Arbitrary Code - SecurityTracker	Third Party Advisory www.securitytracker.com text/html	SECTRACK 1035981
Issue 606185 - chromium - An open-source project to help move the web forward. - Monorail	Permissions Required crbug.com text/html	CONFIRM crbug.com/606185
[security-announce] openSUSE-SU-2016:1430-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1430
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2016:1190
USN-2992-1: Oxide vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2992-1

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	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	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	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	13.2	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

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

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:14.04:*:*:*:lts:*:*:*:

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:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise:12.0:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise:12.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→