



CVE-2013-6644

Published on: 01/16/2014 12:00:00 AM UTC

Last Modified on: 11/10/2022 08:10:00 PM UTC

CVE-2013-6644

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Mac Os X](#) from [Apple](#) contain the following vulnerability:

Multiple unspecified vulnerabilities in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.

CVE-2013-6644 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

[security-announce] openSUSE-SU-2014:0243-1: important: chromium to 32.0

[Mailing List](#)
[Third Party Advisory](#)
[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2014:0243](#)

327729 - chromium - An open-source project to help move the web forward. - Monorail

[Exploit](#)
[Mailing List](#)
[Vendor Advisory](#)
[code.google.com](#)
[text/html](#)

[CONFIRM](#)
[code.google.com/p/chromium/issues/detail?id=327729](#)

Issue 328456 - chromium - ASSERTION FAILED: Im_deletionHasBegun, UNKNOWN in WebCore::FormAssociatedElement::formRemovedFromTree - An open-source project to help move the web forward. - Google Project Hosting

[Exploit](#)
[Mailing List](#)
[Vendor Advisory](#)
[code.google.com](#)
[text/html](#)

[CONFIRM](#)
[code.google.com/p/chromium/issues/detail?id=328456](#)

Issue 322662 - chromium - Multiprofile: Screen does not lock when non-corp account is active - An open-source project to help move the web forward. - Google Project Hosting	Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=322662
317097 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=317097
Sign in - Google Accounts	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=318791
317485 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=317485
304547 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=304547
316298 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=316298
Chrome Releases: Stable Channel Update	Release Notes Vendor Advisory googlechromereleases.blogspot.com text/html	 CONFIRM googlechromereleases.blogspot.com/2014/channel-update.html
313743 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=313743
Issue 333036 - chromium - Tracking bug for internal security fixes for Chrome 32, Release 0 - An open-source project to help move the web forward. - Google Project Hosting	Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=333036
Issue 317284 - chromium - ASSERTION FAILED: width == frameRect.width(), UNKNOWN in WebCore::WEBPImageDecoder::applyPostProcessing - An open-source project to help move the web forward. - Google Project Hosting	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=317284
319477 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=319477
Issue 280352 - chromium - ASSERTION FAILED: !node node->hasTagName(HTMLNames::tdTag) node->hasTagName(HTMLNames::thTag), UNKNOWN in WebCore::AccessibilityTable::isDataTable - An open-source	Exploit Mailing List Vendor Advisory code.google.com	 CONFIRM code.google.com/p/chromium/issues/detail?id=280352

322195 - chromium - An open-source project to help move the web forward. - Google Project Hosting	Exploit text/html	
322195 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=322195
317423 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=317423
320344 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=320344
Issue 314402 - chromium - UNKNOWN in WebCore::computeShapePaddingBounds - An open-source project to help move the web forward. - Google Project Hosting	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=314402
Issue 324321 - chromium - Heap-use-after-free in WebCore::Document::updateLayout - An open-source project to help move the web forward. - Google Project Hosting	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=324321
Debian -- Security Information -- DSA-2862-1 chromium-browser	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-2862
269837 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Mailing List Vendor Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=269837

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All

System						
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
cpe:2.3:o:apple:mac_os_x:*****:						
cpe:2.3:o:apple:mac_os_x:-:*****:						
cpe:2.3:o:apple:mac_os_x:*****:						
cpe:2.3:o:debian:debian_linux:7.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:7.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:a:google:chrome:*****:						
cpe:2.3:a:google:chrome:*****:						

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*.*
cpe:2.3:o:linux:linux_kernel:-:*:*:*:*.*
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*.*
cpe:2.3:o:microsoft:windows:*:*:*:*:*.*
cpe:2.3:o:microsoft:windows:-:*:*:*:*.*
cpe:2.3:o:microsoft:windows:*:*:*:*:*.*
cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*.*
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*.*
cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*.*
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*.*

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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