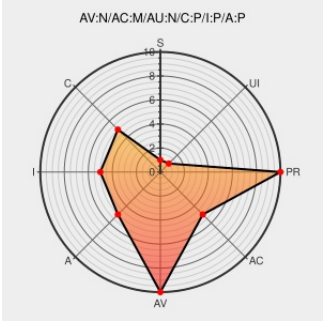
CVE-2013-6645

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

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

CVE-2013-6645

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



Certain versions of Mac Os X from Apple contain the following vulnerability:

Use-after-free vulnerability in the OnWindowRemovingFromRootWindow function in content/browser/web_contents/web_contents_view_aura.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving certain print-preview and tab-switch actions that interact with a speech input element.

CVE-2013-6645 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
320183 - chromium - An open-source project to help move the web forward. - Monorail	Broken Link, code.google.com, text/html	MISC code.google.com/p/chromium/issues/detail?id=320183
[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
Sign in - Google Accounts	Exploit, Mailing List, Vendor Advisory	CONFIRM code.google.com/p/chromium/issues/detail?id=318791

	code.google.com text/html	
Chrome Releases: Stable Channel Update	Release Notes Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2014/01/stable-channel-update.html
[chrome] Revision 235302	Patch Vendor Advisory src.chromium.org text/html	CONFIRM src.chromium.org/viewvc/chrome?revision=235302&view=revision
Debian -- Security Information -- DSA-2862-1 chromium-browser	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-2862

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
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

System						
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 and Source URL Uptime Status status.cve.report