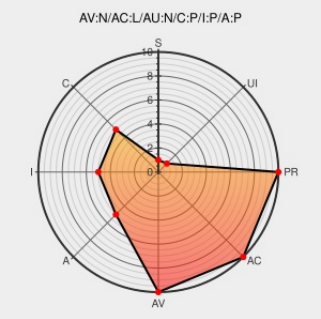
CVE-2014-1718

Published on: 04/09/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:47 PM UTC

CVE-2014-1718

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



Certain versions of Chrome from Google contain the following vulnerability:

Integer overflow in the SoftwareFrameManager::SwapToNewFrame function in content/browser/renderer_host/software_frame_manager.cc in the software compositor in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted mapping of a large amount of renderer memory.

CVE-2014-1718 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
[chrome] Revision 257417	src.chromium.org text/html	CONFIRM src.chromium.org/viewvc/chrome?revision=257417&view=revision
Gentoo Linux Documentation -- Chromium: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-201408-16
[chrome] Revision 258418	src.chromium.org text/html	CONFIRM src.chromium.org/viewvc/chrome?revision=258418&view=revision
Issue 348332 - chromium - Security: Integer overflow allocating shared memory in SoftwareFrameManager::SwapToNewFrame() - 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=348332

openSUSE-SU-2014:0601-1: moderate: update for chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0601
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2014/04/stable-channel-update.html
[chrome] Revision 261817	src.chromium.org text/html	CONFIRM src.chromium.org/viewvc/chrome?revision=261817&view=revision
Debian -- Security Information -- DSA-2905-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-2905
[chrome] Revision 260969	src.chromium.org text/html	CONFIRM src.chromium.org/viewvc/chrome?revision=260969&view=revision

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→