

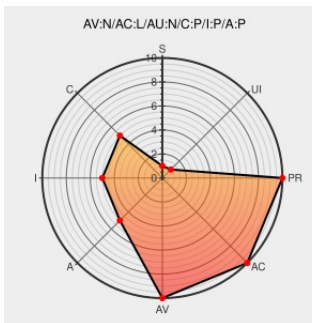


CVE-2014-1720

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

Last Modified on: 03/23/2021 11:25:48 PM UTC

CVE-2014-1720

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

Certain versions of [Chrome](#) from [Google](#) contain the following vulnerability:

Use-after-free vulnerability in the HTMLBodyElement::insertedInto function in core/html/HTMLBodyElement.cpp in Blink, as used 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 involving attributes.

CVE-2014-1720 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

Gentoo Linux Documentation -- Chromium: Multiple vulnerabilities

[security.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-201408-16](#)

[blink] Revision 170216

[src.chromium.org](#)
[text/html](#)

[CONFIRM src.chromium.org/viewvc/blink?revision=170216&view=revision](#)

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](#)

Issue 356095 - chromium - Heap-use-after-free in WebCore::HTMLBodyElement::insertedInto -

[code.google.com](#)
[text/html](#)

[CONFIRM code.google.com/p/chromium/issues/detail?id=356095](#)

Id=356095

www.debian.org

Deprecated Link

text/html



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
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→

© 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