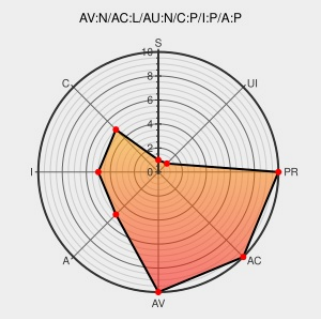
CVE-2011-1796

Published on: 12/25/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:16 PM UTC

CVE-2011-1796

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



Certain versions of Chrome from Google contain the following vulnerability:

Use-after-free vulnerability in the FrameView::calculateScrollbarModesForLayout function in page/FrameView.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that calls the removeChild method during interaction with a FRAME element.

CVE-2011-1796 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
Bug #778822 “11.0.696.57 -> 11.0.696.65” : Bugs : chromium-browser package : Ubuntu	launchpad.net, text/html	CONFIRM launchpad.net/bugs/778822
79055 - chromium - An open-source project to help move the web forward. - Monorail	Vendor Advisory, crbug.com, text/html	CONFIRM crbug.com/79055
Changeset 84300 – WebKit	trac.webkit.org, text/html	CONFIRM trac.webkit.org/changeset/84300

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
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 and Source URL Uptime Status status.cve.report