



CVE-2011-1798

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

Last Modified on: 03/23/2021 11:23:15 PM UTC

CVE-2011-1798

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

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

rendering/svg/RenderSVGText.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 does not properly perform a cast of an unspecified variable during an attempt to handle a block child, which allows remote attackers to cause a denial of service (application crash) or possibly have unknown other impact via a crafted text element in an SVG document.

CVE-2011-1798 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
79595 - chromium - An open-source project to help move the web forward. - Monorail	Vendor Advisory crbug.com text/html	CONFIRM crbug.com/79595
Changeset 84085 – WebKit	trac.webkit.org text/html	CONFIRM trac.webkit.org/changeset/84085

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

CVE Report 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 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