



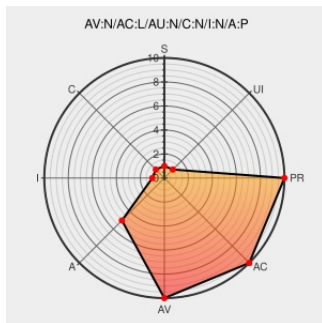
Last Modified on: 03/23/2021 11:23:14 PM UTC

CVE-2011-1691

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

The counterToCSSValue function in CSSComputedStyleDeclaration.cpp in the Cascading Style Sheets (CSS) implementation in WebCore in WebKit before r82222, as used in Google Chrome before 11.0.696.43 and other products, does not properly handle access to the (1) counterIncrement and (2) values of CSSStyleDeclaration data provided by a getComputedStyle allows remote attackers to cause a denial of service (NULL pointer dereference crash) via crafted JavaScript code.

CVE-2011-1691 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Bug 57266 – getComputedStyle counterIncrement crash @ WebCore::counterToCSSValue	Exploit Issue Tracking Patch Third Party Advisory bugs.webkit.org text/html	 CONFIRM bugs.webkit.org/show_bug.cgi?id=57266
Issue 77665 - chromium - getComputedStyle counterIncrement crash @ WebCore::counterToCSSValue - An open-source	Exploit Issue Tracking Patch	 CONFIRM code.google.com/p/chromium/issues/detail?id=77665

project to help move the web forward. - Google Project Hosting	Vendor Advisory code.google.com text/html	
Google Chrome Releases: Beta Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	 CONFIRM googlechromereleases.blogspot.com/2011/04/beta-channel-update_12.html
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	 XF google-countertocssvalue-dos(66818)
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:14365
Changeset 82222 – WebKit	Patch trac.webkit.org text/html	 CONFIRM trac.webkit.org/changeset/82222

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
Application	Google	Chrome	All	All	All	All
cpe:2.3:a:google:chrome:*****:.*						
cpe:2.3:a:google:chrome:*****:.*						

No vendor comments have been submitted for this CVE