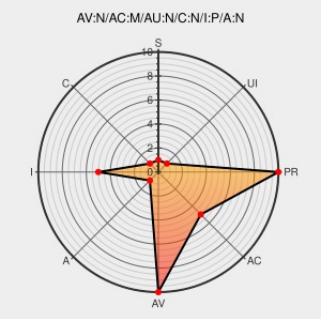
CVE-2009-1413

Published on: 04/24/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:26 PM UTC

CVE-2009-1413

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



Certain versions of Chrome from Google contain the following vulnerability:

Google Chrome 1.0.x does not cancel timeouts upon a page transition, which makes it easier for attackers to conduct Universal XSS attacks by calling setTimeout to trigger future execution of JavaScript code, and then modifying document.location to arrange for JavaScript execution in the context of an arbitrary web site. NOTE: this can be leveraged for a remote attack by exploiting a chromehtml: argument-injection vulnerability.

CVE-2009-1413 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Issue 9860 - chromium - ChromeHTML URI handler vulnerability - Google Code	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=9860
Error 404 (Not Found)!!1	Vendor Advisory chromium.googlecode.com text/html Inactive Link Not Archived	MISC chromium.googlecode.com/issues/attachment?aid=5579180911289877192&name=Google+Chrome+Advisory.doc
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF googlechrome-settimeout-xss(50447)

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	1.0.154.36	All	All	All
Application	Google	Chrome	1.0.154.39	All	All	All
Application	Google	Chrome	1.0.154.42	All	All	All
Application	Google	Chrome	1.0.154.43	All	All	All
Application	Google	Chrome	1.0.154.46	All	All	All
Application	Google	Chrome	1.0.154.53	All	All	All
Application	Google	Chrome	1.0.154.59	All	All	All
Application	Google	Chrome	1.0.154.36	All	All	All
Application	Google	Chrome	1.0.154.39	All	All	All
Application	Google	Chrome	1.0.154.42	All	All	All
Application	Google	Chrome	1.0.154.43	All	All	All
Application	Google	Chrome	1.0.154.46	All	All	All
Application	Google	Chrome	1.0.154.53	All	All	All
Application	Google	Chrome	1.0.154.59	All	All	All

cpe:2.3:a:google:chrome:1.0.154.36:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.39:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.42:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.43:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.46:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.53:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.59:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.36:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.39:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.42:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.43:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.46:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.53:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:1.0.154.59:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→