



CVE-2009-3011

Published on: 08/31/2009 12:00:00 AM UTC

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

CVE-2009-3011

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

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

Google Chrome 1.0.154.48 and earlier, 2.0.172.28, 2.0.172.37, and 3.0.193.2 Beta does not properly block data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header. NOTE: the JavaScript executes outside of the context of the HTTP site.

CVE-2009-3011 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description	Tags	Link
Cross-Site Scripting уразливості в Mozilla, Firefox та Chrome - Websecurity - Веб безпека	Exploit websecurity.com.ua text/html	MISC websecurity.com.ua/3315/
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF googlechrome-data-xss(52998)
Cross-Site Scripting attacks via redirectors - Websecurity - Веб безпека	Exploit websecurity.com.ua text/html	MISC websecurity.com.ua/3386/

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	0.2.149.27	All	All	All
Application	Google	Chrome	0.2.149.29	All	All	All
Application	Google	Chrome	0.2.149.30	All	All	All
Application	Google	Chrome	0.2.152.1	All	All	All
Application	Google	Chrome	0.2.153.1	All	All	All
Application	Google	Chrome	0.3.154.0	All	All	All
Application	Google	Chrome	0.3.154.3	All	All	All
Application	Google	Chrome	0.4.154.18	All	All	All
Application	Google	Chrome	0.4.154.22	All	All	All
Application	Google	Chrome	0.4.154.31	All	All	All
Application	Google	Chrome	0.4.154.33	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	2.0.172.28	All	All	All
Application	Google	Chrome	2.0.172.37	All	All	All
Application	Google	Chrome	3.0.193.2	beta	All	All
Application	Google	Chrome	0.2.149.27	All	All	All
Application	Google	Chrome	0.2.149.29	All	All	All
Application	Google	Chrome	0.2.149.30	All	All	All
Application	Google	Chrome	0.2.152.1	All	All	All
Application	Google	Chrome	0.2.153.1	All	All	All
Application	Google	Chrome	0.3.154.0	All	All	All
Application	Google	Chrome	0.3.154.3	All	All	All
Application	Google	Chrome	0.4.154.18	All	All	All
Application	Google	Chrome	0.4.154.22	All	All	All
Application	Google	Chrome	0.4.154.31	All	All	All
Application	Google	Chrome	0.4.154.33	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	2.0.172.28	All	All	All
Application	Google	Chrome	2.0.172.37	All	All	All
Application	Google	Chrome	3.0.193.2	beta	All	All

Application	Google	Chrome	0.4.154.31	All	All	All
Application	Google	Chrome	0.4.154.33	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	2.0.172.28	All	All	All
Application	Google	Chrome	2.0.172.37	All	All	All
Application	Google	Chrome	3.0.193.2	beta	All	All
Application	Google	Chrome	All	All	All	All
cpe:2.3:a:google:chrome:0.2.149.27:*****:.*:						
cpe:2.3:a:google:chrome:0.2.149.29:*****:.*:						
cpe:2.3:a:google:chrome:0.2.149.30:*****:.*:						
cpe:2.3:a:google:chrome:0.2.152.1:*****:.*:						
cpe:2.3:a:google:chrome:0.2.153.1:*****:.*:						
cpe:2.3:a:google:chrome:0.3.154.0:*****:.*:						
cpe:2.3:a:google:chrome:0.3.154.3:*****:.*:						
cpe:2.3:a:google:chrome:0.4.154.18:*****:.*:						
cpe:2.3:a:google:chrome:0.4.154.22:*****:.*:						
cpe:2.3:a:google:chrome:0.4.154.31:*****:.*:						
cpe:2.3:a:google:chrome:0.4.154.33:*****:.*:						
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:2.0.172.28:*****:.*:						
cpe:2.3:a:google:chrome:2.0.172.37:*****:.*:						
cpe:2.3:a:google:chrome:3.0.193.2:beta:*****:.*:						
cpe:2.3:a:google:chrome:0.2.149.27:*****:.*:						

cpe:2.3:a:google:chrome:0.2.149.29:*****:
cpe:2.3:a:google:chrome:0.2.149.30:*****:
cpe:2.3:a:google:chrome:0.2.152.1:*****:
cpe:2.3:a:google:chrome:0.2.153.1:*****:
cpe:2.3:a:google:chrome:0.3.154.0:*****:
cpe:2.3:a:google:chrome:0.3.154.3:*****:
cpe:2.3:a:google:chrome:0.4.154.18:*****:
cpe:2.3:a:google:chrome:0.4.154.22:*****:
cpe:2.3:a:google:chrome:0.4.154.31:*****:
cpe:2.3:a:google:chrome:0.4.154.33:*****:
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:2.0.172.28:*****:
cpe:2.3:a:google:chrome:2.0.172.37:*****:
cpe:2.3:a:google:chrome:3.0.193.2:beta:*****:
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](#)