



CVE-2009-0411

Published on: 02/03/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:29 PM UTC

CVE-2009-0411

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

Google Chrome before 1.0.154.46 does not properly restrict access from web pages to the (1) Set-Cookie and (2) Set-Cookie2 HTTP response headers, which allows remote attackers to obtain sensitive information from cookies via XMLHttpRequest calls and other web script.

CVE-2009-0411 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

Issue 18533: Merge r5767 - Protect cookie headers from XHR... - Code Review

[codereview.chromium.org](#)
[text/html](#)

CONFIRM [codereview.chromium.org/18533](#)

Issue 11264: Drop Set-Cookie from XHR response headers - Code Review

[codereview.chromium.org](#)
[text/html](#)

CONFIRM [codereview.chromium.org/11264](#)

Release Notes (The Chromium Projects)

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

CONFIRM
[sites.google.com/a/chromium.org/dev/getting-involved/dev-channel/release-notes](#)

[chrome] Revision 8529

[src.chromium.org](#)
[text/html](#)

CONFIRM [src.chromium.org/viewvc/chrome?view=rev&revision=8529](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

XF [googlechrome-xmlhttprequest-info-disclosure\(48554\)](#)

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	0.2.152.1	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	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	All	All	All	All

```
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:*:*:*:*:*:*:
```

```
one:2 3:2 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: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:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)