

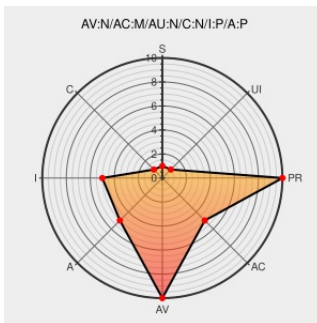


CVE-2008-7294

Published on: 08/09/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:15 PM UTC

CVE-2008-7294

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

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

Google Chrome before 4.0.211.0 cannot properly restrict modifications to cookies established in HTTPS sessions, which allows man-in-the-middle attackers to overwrite or delete arbitrary cookies via a Set-Cookie header in an HTTP response, related to lack of the HTTP Strict Transport Security (HSTS) includeSubDomains feature, aka a "cookie

forcing" issue.

CVE-2008-7294 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Part2 - browsersec - Google Code - Browser Security Handbook, part 2

[code.google.com](#)
[text/html](#)

MISC
[code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies](#)

Security: Cookie forcing

[scarybeastsecurity.blogspot.com](#)
[text/html](#)

MISC
[scarybeastsecurity.blogspot.com/2008/11/cookie-forcing.html](#)

...Application Security...: Cookie Forcing - Trust your cookies no more

[michael-coates.blogspot.com](#)
[text/html](#)

MISC michael-
[coates.blogspot.com/2010/01/cookie-forcing-trust-your-cookies-no.html](#)

Security: Some less obvious benefits of HSTS

[scarybeastsecurity.blogspot.com](#)
[text/html](#)

MISC
[scarybeastsecurity.blogspot.com/2011/02/some-](#)

text/html

www.jacobseccy.blogspot.com/2011/02/some-less-obvious-benefits-of-hsts.html

fyi: Strict Transport Security specification from =JeffH on 2009-09-19 (public-webapps@w3.org from July to September 2009)

lists.w3.org

text/xml

W3 MLIST [public-webapps] 20090918 fyi: Strict Transport Security specification

660053 – (CVE-2011-2976) [SECURITY] If a BUGLIST cookie is compromised, it can be used to XSS show_bug.cgi and inject HTML into

Patch

bugzilla.mozilla.org

text/html

MISC bugzilla.mozilla.org/show_bug.cgi?id=660053

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	0.1.38.1	All	All	All
Application	Google	Chrome	0.1.38.2	All	All	All
Application	Google	Chrome	0.1.38.4	All	All	All
Application	Google	Chrome	0.1.40.1	All	All	All
Application	Google	Chrome	0.1.42.2	All	All	All
Application	Google	Chrome	0.1.42.3	All	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	1.0.154.48	All	All	All

Application	Google	Chrome	1.0.154.48	All	All	All
Application	Google	Chrome	1.0.154.52	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	1.0.154.64	All	All	All
Application	Google	Chrome	1.0.154.65	All	All	All
Application	Google	Chrome	2.0.156.1	All	All	All
Application	Google	Chrome	2.0.157.0	All	All	All
Application	Google	Chrome	2.0.157.2	All	All	All
Application	Google	Chrome	2.0.158.0	All	All	All
Application	Google	Chrome	2.0.159.0	All	All	All
Application	Google	Chrome	2.0.169.0	All	All	All
Application	Google	Chrome	2.0.169.1	All	All	All
Application	Google	Chrome	2.0.170.0	All	All	All
Application	Google	Chrome	2.0.172	All	All	All
Application	Google	Chrome	2.0.172.2	All	All	All
Application	Google	Chrome	2.0.172.27	All	All	All
Application	Google	Chrome	2.0.172.28	All	All	All
Application	Google	Chrome	2.0.172.30	All	All	All
Application	Google	Chrome	2.0.172.31	All	All	All
Application	Google	Chrome	2.0.172.33	All	All	All
Application	Google	Chrome	2.0.172.37	All	All	All
Application	Google	Chrome	2.0.172.38	All	All	All
Application	Google	Chrome	2.0.172.8	All	All	All
Application	Google	Chrome	3.0.182.2	All	All	All
Application	Google	Chrome	3.0.190.2	All	All	All
Application	Google	Chrome	3.0.193.2	beta	All	All
Application	Google	Chrome	3.0.195.2	All	All	All
Application	Google	Chrome	3.0.195.21	All	All	All
Application	Google	Chrome	3.0.195.24	All	All	All
Application	Google	Chrome	3.0.195.25	All	All	All
Application	Google	Chrome	3.0.195.27	All	All	All
Application	Google	Chrome	3.0.195.32	All	All	All
Application	Google	Chrome	3.0.195.33	All	All	All
Application	Google	Chrome	3.0.195.36	All	All	All
Application	Google	Chrome	3.0.195.37	All	All	All

Application	Google	Chrome	0.1.38.1	All	All	All
Application	Google	Chrome	0.1.38.2	All	All	All
Application	Google	Chrome	0.1.38.4	All	All	All
Application	Google	Chrome	0.1.40.1	All	All	All
Application	Google	Chrome	0.1.42.2	All	All	All
Application	Google	Chrome	0.1.42.3	All	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	1.0.154.48	All	All	All
Application	Google	Chrome	1.0.154.52	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	1.0.154.64	All	All	All
Application	Google	Chrome	1.0.154.65	All	All	All
Application	Google	Chrome	2.0.156.1	All	All	All
Application	Google	Chrome	2.0.157.0	All	All	All
Application	Google	Chrome	2.0.157.2	All	All	All
Application	Google	Chrome	2.0.158.0	All	All	All
Application	Google	Chrome	2.0.159.0	All	All	All
Application	Google	Chrome	2.0.169.0	All	All	All
Application	Google	Chrome	2.0.169.1	All	All	All

Application	Google	Chrome	2.0.170.0	All	All	All
Application	Google	Chrome	2.0.172	All	All	All
Application	Google	Chrome	2.0.172.2	All	All	All
Application	Google	Chrome	2.0.172.27	All	All	All
Application	Google	Chrome	2.0.172.28	All	All	All
Application	Google	Chrome	2.0.172.30	All	All	All
Application	Google	Chrome	2.0.172.31	All	All	All
Application	Google	Chrome	2.0.172.33	All	All	All
Application	Google	Chrome	2.0.172.37	All	All	All
Application	Google	Chrome	2.0.172.38	All	All	All
Application	Google	Chrome	2.0.172.8	All	All	All
Application	Google	Chrome	3.0.182.2	All	All	All
Application	Google	Chrome	3.0.190.2	All	All	All
Application	Google	Chrome	3.0.193.2	beta	All	All
Application	Google	Chrome	3.0.195.2	All	All	All
Application	Google	Chrome	3.0.195.21	All	All	All
Application	Google	Chrome	3.0.195.24	All	All	All
Application	Google	Chrome	3.0.195.25	All	All	All
Application	Google	Chrome	3.0.195.27	All	All	All
Application	Google	Chrome	3.0.195.32	All	All	All
Application	Google	Chrome	3.0.195.33	All	All	All
Application	Google	Chrome	3.0.195.36	All	All	All
Application	Google	Chrome	3.0.195.37	All	All	All
Application	Google	Chrome	All	All	All	All
cpe:2.3:a:google:chrome:0.1.38.1:*:*:*:*:*:						
cpe:2.3:a:google:chrome:0.1.38.2:*:*:*:*:*:						
cpe:2.3:a:google:chrome:0.1.38.4:*:*:*:*:*:						
cpe:2.3:a:google:chrome:0.1.40.1:*:*:*:*:*:						
cpe:2.3:a:google:chrome:0.1.42.2:*:*:*:*:*:						
cpe:2.3:a:google:chrome:0.1.42.3:*:*:*:*:*:						
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:1.0.154.48:*****:
cpe:2.3:a:google:chrome:1.0.154.52:*****:
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:1.0.154.64:*****:
cpe:2.3:a:google:chrome:1.0.154.65:*****:
cpe:2.3:a:google:chrome:2.0.156.1:*****:
cpe:2.3:a:google:chrome:2.0.157.0:*****:
cpe:2.3:a:google:chrome:2.0.157.2:*****:
cpe:2.3:a:google:chrome:2.0.158.0:*****:
cpe:2.3:a:google:chrome:2.0.159.0:*****:
cpe:2.3:a:google:chrome:2.0.169.0:*****:
cpe:2.3:a:google:chrome:2.0.169.1:*****:
cpe:2.3:a:google:chrome:2.0.170.0:*****:
cpe:2.3:a:google:chrome:2.0.172:*****:
cpe:2.3:a:google:chrome:2.0.172.2:*****:

cpe:2.3:a:google:chrome:2.0.172.27:*****:
cpe:2.3:a:google:chrome:2.0.172.28:*****:
cpe:2.3:a:google:chrome:2.0.172.30:*****:
cpe:2.3:a:google:chrome:2.0.172.31:*****:
cpe:2.3:a:google:chrome:2.0.172.33:*****:
cpe:2.3:a:google:chrome:2.0.172.37:*****:
cpe:2.3:a:google:chrome:2.0.172.38:*****:
cpe:2.3:a:google:chrome:2.0.172.8:*****:
cpe:2.3:a:google:chrome:3.0.182.2:*****:
cpe:2.3:a:google:chrome:3.0.190.2:*****:
cpe:2.3:a:google:chrome:3.0.193.2:beta:*****:
cpe:2.3:a:google:chrome:3.0.195.2:*****:
cpe:2.3:a:google:chrome:3.0.195.21:*****:
cpe:2.3:a:google:chrome:3.0.195.24:*****:
cpe:2.3:a:google:chrome:3.0.195.25:*****:
cpe:2.3:a:google:chrome:3.0.195.27:*****:
cpe:2.3:a:google:chrome:3.0.195.32:*****:
cpe:2.3:a:google:chrome:3.0.195.33:*****:
cpe:2.3:a:google:chrome:3.0.195.36:*****:
cpe:2.3:a:google:chrome:3.0.195.37:*****:
cpe:2.3:a:google:chrome:0.1.38.1:*****:
cpe:2.3:a:google:chrome:0.1.38.2:*****:
cpe:2.3:a:google:chrome:0.1.38.4:*****:
cpe:2.3:a:google:chrome:0.1.40.1:*****:
cpe:2.3:a:google:chrome:0.1.42.2:*****:
cpe:2.3:a:google:chrome:0.1.42.3:*****:
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:1.0.154.48:*****:
cpe:2.3:a:google:chrome:1.0.154.52:*****:
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:1.0.154.64:*****:
cpe:2.3:a:google:chrome:1.0.154.65:*****:
cpe:2.3:a:google:chrome:2.0.156.1:*****:
cpe:2.3:a:google:chrome:2.0.157.0:*****:
cpe:2.3:a:google:chrome:2.0.157.2:*****:
cpe:2.3:a:google:chrome:2.0.158.0:*****:
cpe:2.3:a:google:chrome:2.0.159.0:*****:
cpe:2.3:a:google:chrome:2.0.169.0:*****:
cpe:2.3:a:google:chrome:2.0.169.1:*****:
cpe:2.3:a:google:chrome:2.0.170.0:*****:
cpe:2.3:a:google:chrome:2.0.170:*****:

cpe:2.3:a:google:chrome:2.0.172.1:*****:
cpe:2.3:a:google:chrome:2.0.172.2:*****:
cpe:2.3:a:google:chrome:2.0.172.27:*****:
cpe:2.3:a:google:chrome:2.0.172.28:*****:
cpe:2.3:a:google:chrome:2.0.172.30:*****:
cpe:2.3:a:google:chrome:2.0.172.31:*****:
cpe:2.3:a:google:chrome:2.0.172.33:*****:
cpe:2.3:a:google:chrome:2.0.172.37:*****:
cpe:2.3:a:google:chrome:2.0.172.38:*****:
cpe:2.3:a:google:chrome:2.0.172.8:*****:
cpe:2.3:a:google:chrome:3.0.182.2:*****:
cpe:2.3:a:google:chrome:3.0.190.2:*****:
cpe:2.3:a:google:chrome:3.0.193.2:beta:*****:
cpe:2.3:a:google:chrome:3.0.195.2:*****:
cpe:2.3:a:google:chrome:3.0.195.21:*****:
cpe:2.3:a:google:chrome:3.0.195.24:*****:
cpe:2.3:a:google:chrome:3.0.195.25:*****:
cpe:2.3:a:google:chrome:3.0.195.27:*****:
cpe:2.3:a:google:chrome:3.0.195.32:*****:
cpe:2.3:a:google:chrome:3.0.195.33:*****:
cpe:2.3:a:google:chrome:3.0.195.36:*****:
cpe:2.3:a:google:chrome:3.0.195.37:*****:
cpe:2.3:a:google:chrome:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)