

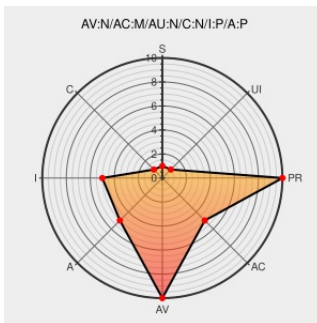


CVE-2008-7298

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

Last Modified on: 03/23/2021 11:25:14 PM UTC

CVE-2008-7298

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

Certain versions of [Android Browser](#) from [Android](#) contain the following vulnerability:

The Android browser in Android 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-2008-7298 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	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.jscssecurity.blogspot.com/2011/02/some-less-obvious-benefits-of-hsts.html

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	Android	Android Browser	All	All	All	All
Application	Android	Android Browser	All	All	All	All
Operating System	Google	Android	All	All	All	All
Operating System	Google	Android	All	All	All	All
cpe:2.3:a:android:android_browser:*****:						
cpe:2.3:a:android:android_browser:*****:						
cpe:2.3:o:google:android:*****:						
cpe:2.3:o:google:android:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →