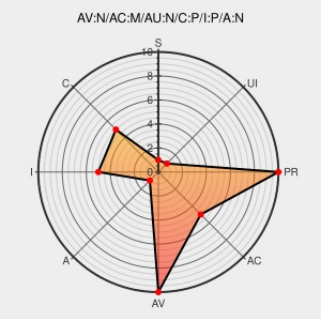
CVE-2009-2060

Published on: 06/15/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:30 PM UTC

CVE-2009-2060

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



Certain versions of Chrome from Google contain the following vulnerability:

src/net/http/http_transaction_winhttp.cc in Google Chrome before 1.0.154.53 uses the HTTP Host header to determine the context of a document provided in a (1) 4xx or (2) 5xx CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.

CVE-2009-2060 has been assigned by 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**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Issue 7338 - chromium - 30x redirects silently honored in response to CONNECT - An open-source project to help move the web forward. - Google Project Hosting	code.google.com text/html	MISC code.google.com/p/chromium/i
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF googlechrome-connect-code-exec
[chrome] Revision 11669	src.chromium.org text/html	CONFIRM src.chromium.org/viewvc/
Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployments - Microsoft Research	research.microsoft.com text/html	MISC research.microsoft.com/apps/p
8473 - chromium - An open-source project to help move the web	code.google.com	MISC code.google.com/p/chromium/i

forward. - Monorail	text/html	
[chrome] Diff of /branches/release_154.next/src/net/http/http_transaction_winhttp.cc	src.chromium.org text/html	CONFIRM src.chromium.org/viewvc/chrome/branch r1=11621&r2=11669&pathrev=11669
479880 – (CVE-2009-1836) Non-200 responses to proxy CONNECT requests lead to attacks on HTTPS	bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.
Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployments - Microsoft Research	research.microsoft.com application/pdf	MISC research.microsoft.com/pubs/7
Release Notes 1.0.154.53 (Chromium Developer Documentation)	web.archive.org text/html Inactive Link Not Archived	CONFIRM sites.google.com/a/chrom notes/releasenotes1015453

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	0.2.149.29	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	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	All	All	All	All

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: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:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→