

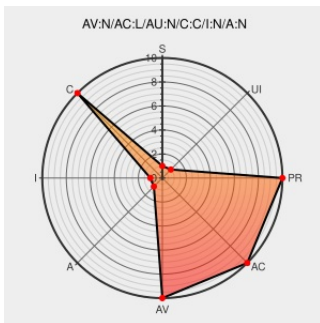


CVE-2009-1412

Published on: 04/24/2009 12:00:00 AM UTC

Last Modified on: 07/23/2021 03:04:00 PM UTC

CVE-2009-1412

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

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

Argument injection vulnerability in the chromehtml: protocol handler in Google Chrome before 1.0.154.59, when invoked by Internet Explorer, allows remote attackers to determine the existence of files, and open tabs for URLs that do not satisfy the IsWebSafeScheme restriction, via a web page that sets document.location to a chromehtml: value, as demonstrated by use of a (1) javascript: or (2) data: URL. NOTE: this can be leveraged for Universal XSS by exploiting certain behavior involving persistence across page transitions.

CVE-2009-1412 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

IBM X-Force Exchange

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

[XF googlechrome-chromehtml-command-execution\(50449\)](#)

Google Chrome Releases: Stable
Update: Security Fix

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

[CONFIRM googlechromereleases.blogspot.com/2009/04/stable-update-security-fix.html](#)

Issue 9860 - chromium -
ChromeHTML URI handler
vulnerability - Google Code

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

[CONFIRM code.google.com/p/chromium/issues/detail?id=9860](#)

Error 404 (Not Found)!!1

[Exploit](#)
[Vendor Advisory](#)

[MISC chromium.googlecode.com/issues/attachment?aid=5579180911289877192&name=Google+Chrome+Advisory.doc](#)

chromium.googlecode.com[text/html](#)

Inactive Link

Not Archived

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	0.2.149.29	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
Application	Microsoft	le	7	All	All	All
Application	Microsoft	le	7	All	All	All
Application	Microsoft	Internet Explorer	7	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:*****:
cpe:2.3:a:microsoft:ie:7:*****:
cpe:2.3:a:microsoft:ie:7:*****:
cpe:2.3:a:microsoft:internet_explorer:7:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)