



Published on: 09/03/2015 12:00:00 AM UTC

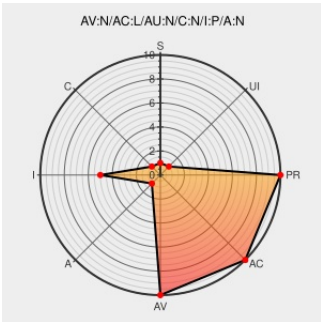
Last Modified on: 11/07/2023 02:24:00 AM UTC

CVE-2015-1296

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

The UnescapeURLWithAdjustmentsImpl implementation in `net/base/escape.cc` in Google Chrome before 45.0.2454.85 does not prevent display of Unicode LOCK characters in the omnibox, which makes it easier for remote attackers to spoof the SSL lock icon by placing one of these characters at the end of a URL, as demonstrated in the following visualizations for right-to-left languages.

CVE-2015-1296 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Chrome Releases: Stable Channel Update	Patch Vendor Advisory googlechromereleases.blogspot.com text/html	 CONFIRM googlechromereleases.blogspot.com/2015/09/stable-channel-update.html
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201603-09
Issue 1189553002: Omnibox: Force text field to LTR context if it is a URL. - Code Review	codereview.chromium.org text/html	 CONFIRM codereview.chromium.org/1189553002/
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:1712

Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, Obtain Potentially Sensitive Information, and Spoof Content - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1033472
openSUSE-SU-2015:1873-1: moderate: Security update for Chromium	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:1873
Issue 421332 - chromium - Security: Completely spoofable origin, including lock sign - Monorail	code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=421332
Issue 1180393003: Added characters that look like padlocks to URL unescaping blacklist. - Code Review	codereview.chromium.org text/html	 CONFIRM codereview.chromium.org/1180393003/
Debian -- Security Information -- DSA-3351-1 chromium-browser	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3351
openSUSE-SU-2015:1586-1: moderate: Security update for Chromium	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:1586

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	All	All	All	All
cpe:2.3:a:google:chrome:*:*:*:*:*.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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