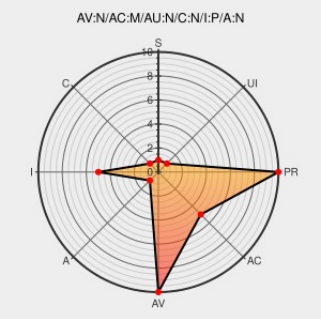
CVE-2015-6790

Published on: 12/14/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

CVE-2015-6790

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



Certain versions of Chrome from Google contain the following vulnerability:

The WebPageSerializerImpl::openTagToString function in WebKit/Source/web/WebPageSerializerImpl.cpp in the page serializer in Google Chrome before 47.0.2526.80 does not properly use HTML entities, which might allow remote attackers to inject arbitrary web script or HTML via a crafted document, as demonstrated by a double-quote character inside a single-quoted string.

CVE-2015-6790 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2015:2291-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2291
USN-2860-1: Oxide vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2860-1
Issue 1398453005: Make WebPageSerializerImpl to escape URL attribute values in result. - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1398453005
Issue 542054 - chromium - Security: properly escaped href attribute leading to offline XSS upon saving a page - ???? ** Chromium issue tracking will soon migrate to	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=542054

tracking will soon migrate to https://bugs.chromium.org (Monorail) ** ???? - Google Project Hosting		
Debian -- Security Information -- DSA-3418-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3418
Google Chrome Prior to 47.0.2526.80 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 78734
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201603-09
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2015/12/stable-channel-update_8.html
[security-announce] openSUSE-SU-2015:2290-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2290
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:2618

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 and Source URL Uptime Status status.cve.report