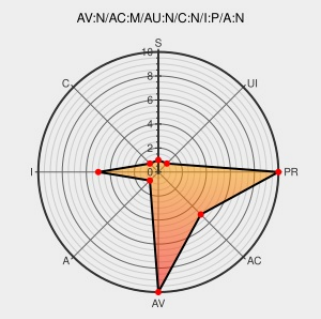
CVE-2015-6786

Published on: 12/05/2015 12:00:00 AM UTC

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

CVE-2015-6786

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



Certain versions of Chrome from Google contain the following vulnerability:

The CSPSourceList::matches function in WebKit/Source/core/frame/csp/CSPSourceList.cpp in the Content Security Policy (CSP) implementation in Google Chrome before 47.0.2526.73 accepts a blob:, data:, or filesystem: URL as a match for a * pattern, which allows remote attackers to bypass intended scheme restrictions in opportunistic circumstances by leveraging a policy that relies on this pattern.

CVE-2015-6786 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
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2015/12/stable-channel-update.html
Debian -- Security Information -- DSA-3415-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3415
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Spoof Content -	www.securitytracker.com text/html	SECTRACK 1034298

SecurityTracker		
Google Chrome Prior to 47.0.2526.73 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 78416
Issue 534570 - chromium - CSP: wildcard source expression (*) should not match data URIs - ???? ** Chromium issue tracking will soon migrate to https://bugs.chromium.org (Monorail) ** ???? - Google Project Hosting	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=534570
Issue 1361763005: Disallow CSP source * matching of data:, blob:, and filesystem: URLs - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1361763005/
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201603-09
[security-announce] openSUSE-SU-2015:2290-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2290
USN-2825-1: Oxide vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2825-1

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→