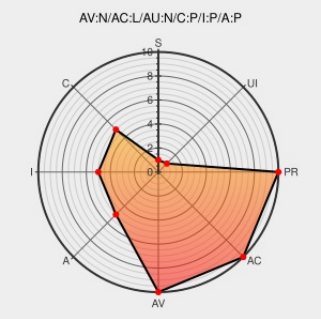
CVE-2015-1302

Published on: 11/11/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1302

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



Certain versions of Chrome from Google contain the following vulnerability:

The PDF viewer in Google Chrome before 46.0.2490.86 does not properly restrict scripting messages and API exposure, which allows remote attackers to bypass the Same Origin Policy via an unintended embedder or unintended plugin loading, related to pdf.js and out_of_process_instance.cc.

CVE-2015-1302 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1841
Debian -- Security Information -- DSA-3415-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3415
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2015/11/stable-channel-update.html
Google Chrome CVE-2015-1302 Information Disclosure Vulnerability	cve.report (archive) text/html	BID 77537

openSUSE-SU-2015:2069-1: moderate: Security update for Chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2069
Issue 1316803003: Prevent leaking PDF data cross-origin - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1316803003
openSUSE-SU-2015:2068-1: moderate: Security update for Chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2068
Google Chrome PDF.js Plugin Flaw Lets Remote Users Obtain Potentially Sensitive Information From Other Domains - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034132
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201603-09
Sign in - Google Accounts	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=520422

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 registred 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