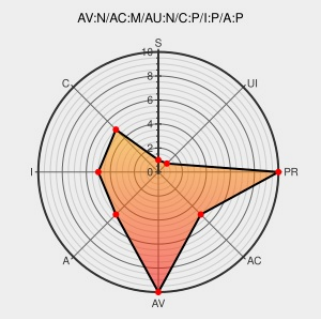
CVE-2015-1245

Published on: 04/19/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:09 PM UTC

CVE-2015-1245

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

Use-after-free vulnerability in the OpenPDFInReaderView::Update function in browser/ui/views/location_bar/open_pdf_in_reader_view.cc in Google Chrome before 41.0.2272.76 might allow user-assisted remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering interaction with a PDFium "Open PDF in Reader" button that has an invalid tab association.

CVE-2015-1245 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3238-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3238
Issue 831283002: Hide the "Open PDF in Reader" bubble on navigations. - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/831283002
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Bypass Same-Origin Restrictions - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1032209
openSUSE-SU-2015:0748-1: moderate: Security update for Chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:0748

Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:0816
openSUSE-SU-2015:1887-1: moderate: Security update for chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1887
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2015/04/stable-channel-update_14.html
Issue 444957 - chromium - Heap-use-after-free in OpenPDFInReaderBubbleView::ButtonPressed - An open-source project to help move the web forward. - Google Project Hosting	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=444957
Chromium: Multiple vulnerabilities (GLSA 201506-04) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201506-04

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Google	Chrome	All	All	All	All

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report