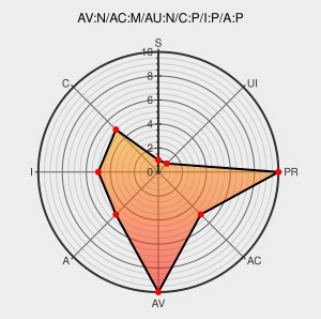
CVE-2015-6756

Published on: 10/15/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6756

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



Certain versions of Chrome from Google contain the following vulnerability:

Use-after-free vulnerability in the CPDFSDK_PageView implementation in fpdfsdk/src/fsdk_mgr.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by leveraging mishandling of a focused annotation in a PDF document.

CVE-2015-6756 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
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Obtain Potentially Sensitive Information - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1033816
Google Chrome 46.0.2490.71 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 77071
Issue 1332653002: Merge to XFA:Fix heap use after free in CPDFSDK_Annot::GetPDFAnnot. - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1332653002
Red Hat Customer Portal	web.archive.org text/html	REDHAT RHSA-2015:1912

	Inactive Link Not Archived	
Chrome Releases: Stable Channel Update	Patch Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2015/10/stable-channel-update.html
507316 - chromium - An open-source project to help move the web forward. - Monorail	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=507316
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201603-09
Debian -- Security Information -- DSA-3376-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3376

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→