



CVE-2016-5140

Published on: 08/07/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:09 PM UTC

CVE-2016-5140

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Chrome](#) from [Google](#) contain the following vulnerability:

Heap-based buffer overflow in the `opj_j2k_read_SQcd_SQcc` function in `j2k.c` in OpenJPEG, as used in PDFium in Google Chrome before 52.0.2743.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JPEG 2000 data.

CVE-2016-5140 has been assigned by [security@google.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

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
Issue 2071773002: openjpeg: Prevent a buffer overflow in <code>opj_j2k_read_SQcd_SQcc</code> . - Code Review	Patch codereview.chromium.org text/html	CONFIRM codereview.chromium.org/2071773002
[security-announce] openSUSE-SU-2016:1982-	lists.opensuse.org	SUSE openSUSE-SU-2016:1982

1: important: Security update	text/html	
Google Chrome Prior to 52.0.2743.116 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 92276
Chromium: Multiple vulnerabilities (GLSA 201610-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201610-09
Google Chrome Multiple Flaws Lets Remote Users Bypass Same-Origin Restrictions, Spoof URLs, and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTrack 1036547
619405 - chromium - An open-source project to help move the web forward. - Monorail	Permissions Required cbug.com text/html	CONFIRM cbug.com/619405
[security-announce] openSUSE-SU-2016:1983-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1983
[SECURITY] Fedora 24 Update: chromium-52.0.2743.116-1.fc24 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2016-e9798eaaa3
Debian -- Security Information -- DSA-3645-1 chromium-browser	www.debian.org Deprecated Link text/html	DEBIAN DSA-3645
Chrome Releases: Stable Channel Update for Desktop	Release Notes googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop.html
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1580

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 →](#)

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 registered 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](#)