



CVE-2014-7901

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-7901
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-19 11:59:00 UTC
Updated	2023-11-07 02:21:00 UTC
Description	Integer overflow in the opj_t2_read_packet_data function in fxcodec/fx_libopenjpeg/libopenjpeg20/t2.c in OpenJPEG in PDF

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All

References

Reference	Source	Link
Sign in - Google Accounts	CONFIRM	code.google.com
e93d5341d87c54713a9632c8823288fa901a3b78 - pdfium - Git at Google	CONFIRM	pdfium.google.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code and Obtain Information - SecurityTracker		www.securitytracker.com
Chrome Releases: Stable Channel Update	CONFIRM	googlechrome.blogspot.com
Google Chrome CVE-2014-7901 Integer Overflow Vulnerability		www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)