



CVE-2014-7900

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

Summary

CVE	CVE-2014-7900
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	Use-after-free vulnerability in the CPDF_Parser::IsLinearizedFile function in fpdfapi/fpdf_parser/fpdf_parser_parser.cpp in F

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
Issue 406868 - chromium - Heap-use-after-free in CPDF_Object::Release - An open-source project to help move the web forward. - Google P
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code and Obtain Information - SecurityTracker
Chrome Releases: Stable Channel Update
Google Chrome CVE-2014-7900 Use After Free Remote Code Execution Vulnerability
IBM X-Force Exchange
1b04ea3b0fb3ae3be3ae6b3824c5e0dad0e73d44 - pdfium - Git at Google
CVE Program record
NVD vulnerability detail

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](#)