CVE-2016-5157

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-5157
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-11 10:59:13 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Heap-based buffer overflow in the opj_dwt_interleave_v function in dwt.c in OpenJPEG, as used in PDFium in Google Chrc

Risk And Classification

Primary CVSS: v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.065920000 probability, percentile 0.912200000 (date 2026-05-06)

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
[SECURITY] Fedora 24 Update: mingw-openjpeg2-2.1.1-3.fc24 - package-announce - Fedora Mailing-Lists
Chrome Releases: Stable Channel Update for Desktop
Chromium: Multiple vulnerabilities (GLSA 201610-09) — Gentoo security
[SECURITY] Fedora 24 Update: openjpeg2-2.1.1-3.fc24 - package-announce - Fedora Mailing-Lists
Bug 1374337 – openjpeg: Heap buffer overflow in opj_dwt_interleave_v in dwt.c

Red Hat Customer Portal
Add sanity check for tile coordinates (#823) · uclouvain/openjpeg@e078172 · GitHub
openSUSE-SU-2016:2349-1: moderate: Security update for opera
Debian -- Security Information -- DSA-3660-1 chromium-browser
[SECURITY] Fedora 23 Update: openjpeg2-2.1.1-3.fc23 - package-announce - Fedora Mailing-Lists
[security-announce] SUSE-SU-2016:2251-1: important: Security update for
oss-security - Re: CVE Request: OpenJPEG Heap Buffer Overflow Issue
b6befb2ed2485a3805cddea86dc7574510178ea9 - pdfium - Git at Google
Google Chrome Prior to 53.0.2785.89 Multiple Security Vulnerabilities
[SECURITY] Fedora 23 Update: mingw-openjpeg2-2.1.1-3.fc23 - package-announce - Fedora Mailing-Lists
[security-announce] openSUSE-SU-2016:2296-1: important: Security update
632622 - chromium - An open-source project to help move the web forward. - Monorail
[SECURITY] Fedora 25 Update: openjpeg2-2.1.1-3.fc25 - package-announce - Fedora Mailing-Lists
[security-announce] openSUSE-SU-2016:2250-1: important: Security update
Debian -- Security Information -- DSA-4013-1 openjpeg2
[SECURITY] Fedora 25 Update: mingw-openjpeg2-2.1.1-3.fc25 - package-announce - Fedora Mailing-Lists
Google Chrome Multiple Flaws Lets Remote Users Bypass Security Restrictions, Conduct Cross-Site Scripting Attacks, Spoof URLs, and Exe
[SECURITY] Fedora 23 Update: openjpeg2-2.1.1-3.fc23 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 24 Update: openjpeg2-2.1.1-3.fc24 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 24 Update: mingw-openjpeg2-2.1.1-3.fc24 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 25 Update: mingw-openjpeg2-2.1.1-3.fc25 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 23 Update: mingw-openjpeg2-2.1.1-3.fc23 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 25 Update: openjpeg2-2.1.1-3.fc25 - package-announce - Fedora Mailing-Lists
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.

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