libjxl: Uninitialized memory read in decoder due to incorrect optimization in patch handling

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

Summary

CVE	CVE-2025-12474
State	PUBLISHED
Assigner	Google
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-11 16:15:53 UTC
Updated	2026-04-24 16:42:18 UTC
Description	A specially-crafted file can cause libjxl's decoder to read pixel data from uninitialized (but allocated) memory. This can be d

Risk And Classification

Primary CVSS: v4.0 2.3 LOW from cve-coordination@google.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000060000 probability, percentile 0.003380000 (date 2026-04-26)

Problem Types: CWE-908 | CWE-908 CWE-908 Use of Uninitialized Resource

Version	Source	Type	Score	Severity	Vector
4.0	cve-coordination@google.com	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N
4.0	CNA	CVSS	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N
3.1	nvd@nist.gov	Primary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libjxl Project	Libjxl	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Google	Libjxl	affected 0.7 0.11.1 semver	Not specified

References

Reference	Source	Link	Tags
github.com/libjxl/libjxl/pull/4495	cve-coordination@google.com	github.com	Issue Tracking, Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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