lz4_flex: Decompression can leak information from uninitialized memory or reused output buffer

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-32829
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-20 01:15:56 UTC
Updated	2026-03-30 15:05:23 UTC
Description	lz4_flex is a pure Rust implementation of LZ4 compression/decompression. In versions 0.11.5 and below, and 0.12.0, deco

Risk And Classification

Primary CVSS: v4.0 8.2 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/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: 0.000150000 probability, percentile 0.031570000 (date 2026-04-01)

Problem Types: CWE-201 | CWE-823 | CWE-201 CWE-201: Insertion of Sensitive Information Into Sent Data | CWE-823 CWE-823: Use of Out-of-range Pointer Offset

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/S
4.0	CNA	DECLARED	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/S
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pseitz	Lz4 Flex	All	All	All	All
Application	Pseitz	Lz4 Flex	0.12.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	PSeitz	Lz4 Flex	affected < 0.11.6	Not specified
CNA	PSeitz	Lz4 Flex	affected >= 0.12.0, < 0.12.1	Not specified

References

Reference	Source	Link	Tags
rustsec.org/advisories/RUSTSEC-2026-0041.html	security-advisories@github.com	rustsec.org	Third
github.com/PSeitz/lz4_flex/commit/055502ee5d297ecd6bf448ac91c055c7f6df9b6d	security-advisories@github.com	github.com	Patch
github.com/PSeitz/lz4_flex/security/advisories/GHSA-vvp9-7p8x-rfvv	security-advisories@github.com	github.com	Mitiga
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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