GCM chunking can lead to bad tag exception on decryption

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

Summary

CVE	CVE-2026-8149
State	PUBLISHED
Assigner	bcorg
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 07:16:29 UTC
Updated	2026-05-08 07:16:29 UTC
Description	A vulnerability in Legion of the Bouncy Castle Inc. BC-FJA BC-FIPS on Linux, X86_64, AVX, AVX-512f. This vulnerability is

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from 91579145-5d7b-4cc5-b925-a0262ff19630

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/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:N/AU:X/R:X/V:X/RE:M/U:Amber

Problem Types: CWE-1068 | CWE-1068 CWE-1068

Version	Source	Type	Score	Severity	Vector
4.0	91579145-5d7b-4cc5-b925-a0262ff19630	Secondary	5.1	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

ntegrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/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:N/AU:X/R:X/V:X/RE:M/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Legion Of The Bouncy Castle Inc.	BC-FJA	affected 2.1.0 2.1.2 maven	Linux, X86_64, AVX, AVX-512f

References

Reference	Source	Link	Tags
do-not-publish.bouncycastle.org/do_not_publish	91579145-5d7b-4cc5-b925-a0262ff19630	do-not-publish.bouncycastle.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: Michael Schäfer, Kiteworks (en)

Additional Advisory Data

Workarounds

CNA: If possible pass whole message to GCM via doFinal(..) for decryption. Issue only occurs when decryption is chunked at certain boundaries.

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