



# GCM chunking can lead to bad tag exception on decryption

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

## Summary

<b>CVE</b>	CVE-2026-8149
<b>State</b>	PUBLISHED
<b>Assigner</b>	bcorg
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 07:16:29 UTC
<b>Updated</b>	2026-05-08 07:16:29 UTC
<b>Description</b>	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/MSX/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

Integrity

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/MSX: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	<a href="#">Legion Of The Bouncy Castle Inc.</a>	<a href="#">BC-FJA</a>	affected 2.1.0 2.1.2 maven	Linux, X86_64, AVX, AVX-512f

### References

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)