Unbounded PGP AEAD chunk size leads to pre-auth resource exhaustion.

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

Summary

CVE	CVE-2026-3505
State	PUBLISHED
Assigner	bcorg
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 10:16:49 UTC
Updated	2026-04-21 17:16:53 UTC
Description	Allocation of resources without limits or throttling, Uncontrolled Resource Consumption vulnerability in Legion of the Bouncy

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from 91579145-5d7b-4cc5-b925-a0262ff19630

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/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: 0.000550000 probability, percentile 0.174420000 (date 2026-04-22)

Problem Types: CWE-400 | CWE-770 | CWE-770 CWE-770 Allocation of resources without limits or throttling | CWE-400 CWE-400 Uncontrolled Resource Consumption

Version	Source	Type	Score	Severity	Vector
4.0	91579145-5d7b-4cc5-b925-a0262ff19630	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Legion Of The Bouncy Castle Inc.	BC-JAVA	affected 1.74 1.84 maven	all

References

Reference	Source	Link
github.com/bcgit/bc-java/wiki/CVE%E2%80%902026%E2%80%903505	91579145-5d7b-4cc5-b925-a0262ff19630	github.com
github.com/bcgit/bc-java/commit/dc7530939ffb6cdb57636f3609d98e23b94e71c1	91579145-5d7b-4cc5-b925-a0262ff19630	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Disclosure <disclosure@aisle.com> (en)

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**