



Non-constant time comparisons risk private key leakage in FrodoKEM.

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

Summary

CVE	CVE-2026-5598
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 16:16:20 UTC
Description	Covert timing channel vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA core on all (core modules). This vulnerabil

Risk And Classification

Primary CVSS: v4.0 8.9 HIGH from 91579145-5d7b-4cc5-b925-a0262ff19630

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N/E:U/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:P/AU:Y/R:X/V:X/RE:X/U:R
ed

EPSS: 0.000180000 probability, percentile 0.047780000 (date 2026-04-22)

Problem Types: CWE-385 | CWE-385 CWE-385 Covert timing channel

Version	Source	Type	Score	Severity	Vector
4.0	91579145-5d7b-4cc5-b925-a0262ff19630	Secondary	8.9	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N/E:U/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:P/AU:Y/R:X/V:X/RE:X/U:R
4.0	CNA	CVSS	8.9	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N/E:U/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:P/AU:Y/R:X/V:X/RE:X/U:R

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N/E:U/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:P/AU:Y/R:X/V:X/RE:X/U:R
ed



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Legion Of The Bouncy Castle Inc.	BC-JAVA	affected 1.71 1.84 maven	all

References

Reference	Source	Link
github.com/bcgit/bc-java/wiki/CVE%E2%80%90902026%E2%80%90905598	91579145-5d7b-4cc5-b925-a0262ff19630	github.com
github.com/bcgit/bc-java/commit/8692e6b2b191fc4aafa32545c7a78bdb9bf110c5	91579145-5d7b-4cc5-b925-a0262ff19630	github.com
github.com/bcgit/bc-java/commit/94abbd56413dfdac651fd878bc60253871ef5e87	91579145-5d7b-4cc5-b925-a0262ff19630	github.com
github.com/bcgit/bc-java/wiki/CVE%E2%80%90902026%E2%80%90905998	MITRE	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



Vendor Comments And Credit

Discovery Credit

CNA: Cristina Dueñas Navarro (cristina.duenas@jtsec.es) (en)

CNA: Sunwoo Lee (sunwoolee@kentech.ac.kr) Woohyun Choi (woohyun@kentech.ac.kr) Seunghyun Yoon (seunghyunyoon@kentech.ac.kr) Korea Institute of Energy Technology (KENTECH) (en)

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

© [CVE.report](#) 2026 |

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)