



# GOSTCTR implementation unable to process more than 255 blocks correctly

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2025-14813   |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | bcorg  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2026-04-15 10:16:38 UTC  |
| <b>Updated</b>         | 2026-04-17 15:38:09 UTC  |
| <b>Description</b>     | Use of a Broken or Risky Cryptographic Algorithm vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA bcprov on all ( |

## Risk And Classification

**Primary CVSS:** v4.0 9.3 CRITICAL from 91579145-5d7b-4cc5-b925-a0262ff19630

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

**EPSS:** 0.000040000 probability, percentile 0.001600000 (date 2026-04-21)

**Problem Types:** CWE-327 | CWE-327 CWE-327: Use of a Broken or Risky Cryptographic Algorithm

| Version | Source                               | Type      | Score | Severity | Vector   |
|---------|--------------------------------------|-----------|-------|----------|--|
| 4.0     | 91579145-5d7b-4cc5-b925-a0262ff19630 | Secondary | 9.3   | CRITICAL | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA |
| 4.0     | CNA                                  | CVSS      | 9.3   | CRITICAL | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA |

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

None

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

#### Vendor Declared Affected Products

| Source | Vendor   | Product | Version                  | Platforms |
|--------|--|---------|--------------------------|-----------|
| CNA    | <a href="#">Legion Of The Bouncy Castle Inc.</a> | BC-JAVA | affected 1.59 1.84 maven | all       |

#### References

| Reference   | Source                               | Link   |
|---|--------------------------------------|--|
| <a href="https://github.com/bcgit/bc-java/commit/b42574345414e4b7c8051b16fa1fafe01c29871f">github.com/bcgit/bc-java/commit/b42574345414e4b7c8051b16fa1fafe01c29871f</a> | 91579145-5d7b-4cc5-b925-a0262ff19630 | <a href="#">github.com</a>                     |
| <a href="https://github.com/bcgit/bc-java/commit/701686cb0184cd9ae103c801b3581fdf95c6d4f3">github.com/bcgit/bc-java/commit/701686cb0184cd9ae103c801b3581fdf95c6d4f3</a> | 91579145-5d7b-4cc5-b925-a0262ff19630 | <a href="#">github.com</a>                     |
| <a href="https://github.com/bcgit/bc-java/wiki/CVE%E2%80%90902025%E2%80%909014813">github.com/bcgit/bc-java/wiki/CVE%E2%80%90902025%E2%80%909014813</a>                 | 91579145-5d7b-4cc5-b925-a0262ff19630 | <a href="#">github.com</a>                     |
| CVE Program record  | CVE.ORG                              | <a href="http://www.cve.org">www.cve.org</a>   |
| NVD vulnerability detail  | NVD                                  | <a href="http://nvd.nist.gov">nvd.nist.gov</a> |

#### Vendor Comments And Credit

Discovery Credit

**CNA:** XlabAI Team of Tencent Xuanwu Lab (en)

**CNA:** Atuin Automated Vulnerability Discovery Engine (en)

**CNA:** Lili Tang, Guannan Wang, and Guancheng Li (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](#)