



Possible DOS in processing large name constraint structures in PKIXCertPathReveiwier

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2025-8916 |
| State | PUBLISHED |
| Assigner | bcorg |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2025-08-13 10:15:27 UTC |
| Updated | 2026-05-12 13:17:29 UTC |
| Description | Allocation of Resources Without Limits or Throttling vulnerability in Legion of the Bouncy Castle Inc. BC Java bcpxk on All (|

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from 91579145-5d7b-4cc5-b925-a0262ff19630

CVSS:4.0/AV:N/AC:L/AT:P/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/MS:C:X/MSI:X/MSA:X/S:P/AU:X/R:U/V:X/RE:M/U:Amber

EPSS: 0.000850000 probability, percentile 0.243940000 (date 2026-05-12)

Problem Types: CWE-770 | CWE-770 CWE-770 Allocation of Resources Without Limits or Throttling

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------------|-----------|-------|----------|---|
| 4.0 | 91579145-5d7b-4cc5-b925-a0262ff19630 | Secondary | 6.3 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA: |
| 4.0 | CNA | CVSS | 6.3 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA: |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

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:N/AC:L/AT:P/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:P/AU:X/R:U/V:X/RE:M/U:Amber

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--|-----------------|----------------------------|---------------|
| CNA | Legion Of The Bouncy Castle Inc. | BC Java | affected 1.44 1.78 maven | All |
| CNA | Legion Of The Bouncy Castle Inc. | BC Java | affected 1.44 1.78 maven | All |
| CNA | Legion Of The Bouncy Castle Inc. | BCPKIX FIPS | affected 1.0.0 1.0.7 maven | All |
| CNA | Legion Of The Bouncy Castle Inc. | BCPKIX FIPS | affected 2.0.0 2.0.7 maven | All |
| ADP | Siemens | SIMATIC CN 4100 | affected V5.0 custom | Not specified |

References

| Reference | Source | Link |
|---|--------------------------------------|---|
| github.com/bcgit/bc-java/wiki/CVE%E2%80%90902025%E2%80%90908916 | 91579145-5d7b-4cc5-b925-a0262ff19630 | github.com |
| cert-portal.siemens.com/productcert/html/ssa-032379.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

Vendor Comments And Credit

Discovery Credit

CNA: Bing Shi (en)

Additional Advisory Data

Workarounds

CNA: Limiting the size of ASN.1 objects that can be loaded from "the wild" will mitigate the risk of an exploit by automatically putting a cap on the maximum size of a Name Constraints structure.

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](#)