

Spring Security Advisories



CVE-2026-40979: ONNX model cache defaults to world-writable predictable /tmp directory

MODERATE | APRIL 27, 2026 | CVE-2026-40979

Description

In Spring AI, having access to a shared environment can expose the ONNX model used by the application.

Only applications that use `TransformersEmbeddingModel` and have the cache enabled, using the default location, are affected.

Affected Spring Products and Versions

Spring AI:

- 1.0.0 - 1.0.x
- 1.1.0 - 1.1.x

Mitigation

Users of affected versions should upgrade to the corresponding fixed version.

| Affected version(s) | Fix version | Availability |
|---------------------|-------------|--------------|
| 1.0.x | 1.0.6 | OSS |
| 1.1.x | 1.1.5 | OSS |

Reporting a vulnerability

To report a security vulnerability for a project within the Spring portfolio, see the [Security Policy](#)

References

- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?version=3.1&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N>

Get ahead

VMware offers training and certification to turbo-charge your progress.

[Learn more](#)

Get support

Tanzu Spring offers support and binaries for OpenJDK™, Spring, and Apache Tomcat® in one simple subscription.

[Learn more](#)

Upcoming events

Check out all the upcoming events in the Spring community.

[View all](#)



Why Spring

- Generative AI
- Microservices
- Reactive
- Event Driven
- Cloud
- Web Applications
- Serverless
- Batch

Learn

- Quickstart
- Guides
- Courses
- Get Certified

Projects

Resources

- Blog
- Release Calendar
- Version Mappings
- Release Highlights

Community

- Events
- Authors
- Enterprise**
- Long-term Support
- Automated Upgrades
- Governance and Compliance

Thank You

Get the Spring newsletter

Stay connected with the Spring newsletter

SUBSCRIBE



Copyright © 2005 - 2026 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

[Terms of Use](#) • [Privacy](#) • [Trademark Guidelines](#)

Apache®, Apache Tomcat®, Apache Kafka®, Apache Cassandra™, and Apache Geode™ are trademarks or registered trademarks of the Apache Software Foundation in the United States and/or other countries. Java™, Java™ SE, Java™ EE, and OpenJDK™ are trademarks of Oracle and/or its affiliates. Kubernetes® is a registered trademark of the Linux Foundation in the United States and other countries. Linux® is the registered trademark of Linus Torvalds in the United States and other countries. Windows® and Microsoft® Azure are registered trademarks of Microsoft Corporation. "AWS" and "Amazon Web Services" are trademarks or registered trademarks of Amazon.com Inc. or its affiliates. All other trademarks and copyrights are property of their respective owners and are only mentioned for informative purposes. Other names may be trademarks of their respective owners.