spring by VMware Tanzu

Spring Security Advisories

RSS feed

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

spring by VMware Tanzu

Thank You

Get the Spring newsletter

Stay connected with the Spring newsletter

SUBSCRIBE

spring by VMware Tanzu