spring by VMware Tanzu

Spring Security Advisories

RSS feed

CVE-2026-40973: Predictable temp directory accepted without ownership verification

HIGH | APRIL 23, 2026 | CVE-2026-40973

Description

A local attacker on the same host as the application may be able to take control of the directory used by `ApplicationTemp`. When `server.servlet.session.persistent` is set to `true` and the attack persists across application restarts, this may allow the attacker to read session information and hijack authenticated users or deploy a gadget chain and execute code as the application's user.

Affected Spring Products and Versions

Spring Boot:

- 4.0.0 - 4.0.5
- 3.5.0 - 3.5.13
- 3.4.0 - 3.4.15
- 3.3.0 - 3.3.18
- 2.7.0 - 2.7.32

Versions that are no longer supported are also affected.

Mitigation

Reporting a vulnerability

To report a security vulnerability for a project within the Spring portfolio, see the Security Policy

spring by VMware Tanzu

Affected version(s)	Fix version	Availability
4.0.x	4.0.6	OSS
3.5.x	3.5.14	OSS
3.4.x	3.4.16	Enterprise Support Only
3.3.x	3.3.19	Enterprise Support Only
2.7.x	2.7.33	Enterprise Support Only

No further mitigation steps are necessary.

References

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

History

- 2026-04-23: Initial vulnerability report published.