spring by VMware Tanzu

Spring Security Advisories

RSS feed

CVE-2026-22751: Spring Security JdbcOneTimeTokenService allows a one-time token to authenticate multiple sessions

MEDIUM | APRIL 21, 2026 | CVE-2026-22751

Reporting a vulnerability

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

Description

Applications that explicitly configure One-Time Token login with `JdbcOneTimeTokenService` are vulnerable to a Time-of-check Time-of-use (TOCTOU) race condition. An attacker with a valid one-time token can send concurrent requests to the authentication endpoint, allowing the single-use token to be consumed multiple times and establishing multiple authenticated sessions. The default `InMemoryOneTimeTokenService` is thread-safe and not affected by this vulnerability.

Affected Spring Products and Versions

Spring Security:

- 6.4.0 - 6.4.15
- 6.5.0 - 6.5.9
- 7.0.0 - 7.0.4

Mitigation

Affected version(s)	Fix version	Availability
6.4.x	6.4.16	Commercial
6.5.x	6.5.10	OSS
7.0.x	7.0.5	OSS

Credit

The issue was identified and responsibly reported by Jinyeong Seol (@Seol-JY).

References

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