spring by VMware Tanzu

Spring Security Advisories

RSS feed

CVE-2026-22747: Unauthorized User Impersonation when Using X.509 Client Certificates

MEDIUM | APRIL 20, 2026 | CVE-2026-22747

Description

`SubjectX500PrincipalExtractor` does not correctly handle certain malformed X.509 certificate `CN` values, which can lead to reading the wrong value for the username. In a carefully crafted certificate, this can lead to an attacker impersonating another user.

Environmental Considerations

This component sits behind Spring Security's pre-authentication flow, which assumes the presented credentials have already been validated by a trusted upstream. Exploiting this issue therefore presupposes a compromise of that upstream trust. So while we recommend upgrading, this fix is better understood as defense-in-depth than as closing a standalone attack path.

Also note that this fix only addresses `SubjectX500PrincipalExtractor` and not `SubjectDnX509PrincipalExtractor`, a deprecated component.

Affected Spring Products and Versions

Spring Security:

Reporting a vulnerability

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

Mitigation

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

Affected version(s)	Fix version	Availability
7.0.x	7.0.5	OSS

Credit

The issue was identified and responsibly reported by Nikita Markevich.

References

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

History

- 2026-04-20: Initial vulnerability report published.