spring by VMware Tanzu

Spring Security Advisories

RSS feed

CVE-2026-22748: Potential Security Misconfiguration when Using withIssuerLocation

MEDIUM | APRIL 20, 2026 | CVE-2026-22748

Description

When an application configures JWT decoding with `NimbusJwtDecoder` or `NimbusReactiveJwtDecoder`, it must configure an `OAuth2TokenValidator<Jwt>` separately, for example by calling `setJwtValidator`.

This is easy to miss when using `NimbusJwtDecoder#withIssuerLocation` or `NimbusReactiveJwtDecoder#withIssuerLocation`, which may be interpreted as adding issuer validation automatically.

Recent maintenance versions of `NimbusJwtDecoder#withIssuerLocation` and `NimbusReactiveJwtDecoder#withIssuerLocation` now add issuer validation by default.

Affected Spring Products and Versions

Spring Security:

- 6.3.0 - 6.3.14
- 6.4.0 - 6.4.14
- 6.5.0 - 6.5.9
- 7.0.0 - 7.0.4
- Older, unsupported versions are also affected.

Mitigation

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

Affected version(s)	Fix version	Availability
6.3.x	6.3.15	Enterprise Support Only
6.4.x	6.4.15	Enterprise Support Only
6.5.x	6.5.10	OSS
7.0.x	7.0.5	OSS

Note that if this upgrade causes you trouble due to unwanted issuer validation, you can change it to the earlier default in the following way:

```
@Bean
JwtDecoder jwtDecoder() {
    String issuer = "https://issuer.example.org";
```

Reporting a vulnerability

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

```
        .build();
    jwtDecoder.setOAuth2TokenValidator(JwtValidators.createDefaults()); // set to t
    return jwtDecoder;
}
```

Credit

The issue was identified and responsibly reported by Daniel Seiler.

References

- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C/CR:L/IR:M/AR:L/MAV:N/MAC:H/MPR:H/MUI:N/MS:C/MC:N/MI:H/MA:N&version=3.1

History

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

SUBSCRIBE