Spring Security Advisories

RSS feed

This page lists Spring advisories.

Reporting a vulnerability

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

CVE-2025-41235: Spring Cloud Gateway Server Forwards Headers from Untrusted Proxies

HIGH | MAY 27, 2025 | CVE-2025-41235

Description

Spring Cloud Gateway Server forwards the `X-Forwarded-For` and `Forwarded` headers from untrusted proxies.

Affected Spring Products and Versions

Spring Cloud Gateway Server:

- 2.2.10.RELEASE - 4.2.2, 4.3.0-{M1, M2, RC1}

Spring Cloud Gateway Server MVC:
...

READ MORE

CVE-2025-41232: Spring Security authorization bypass for method security annotations on private methods

MEDIUM | MAY 19, 2025 | CVE-2025-41232

Description

Spring Security Aspects may not correctly locate method security annotations on private methods. This can cause an authorization bypass.

Your application may be affected by this if the following are true:

1. You are using `@EnableMethodSecurity(mode=ASPECTJ)` and `spring-security-aspects`, and
2. You have Spring Security method annotations on a private method
...

READ MORE

CVE-2025-22233: Spring Framework DataBinder Case Sensitive Match Exception (2nd update)

LOW | MAY 15, 2025 | CVE-2025-22233

Description

CVE-2024-38820 ensured Locale-independent, lowercase conversion for both the configured `disallowedFields` patterns and for request parameter names. However, there are still cases where it is possible to bypass the `disallowedFields` checks.

Affected...

READ MORE

CVE-2025-22235: Spring Boot EndpointRequest.to() creates wrong matcher if actuator endpoint is not exposed

MEDIUM | APRIL 24, 2025 | CVE-2025-22235

Description

`EndpointRequest.to()` creates a matcher for `null/**` if the actuator endpoint, for which the `EndpointRequest` has been created, is disabled or not exposed.

Your application may be affected by this if all the following conditions are met:

- You use Spring Security
- `EndpointRequest.to()` has been used in a Spring Security chain configuration
- The endpoint which `EndpointRequest` references is disabled or not exposed via web
- Your application handles requests to `/null` and this path needs protection

...

READ MORE

CVE-2025-22234: Spring Security BCryptPasswordEncoder maximum password length breaks timing attack mitigation

MEDIUM | APRIL 22, 2025 | CVE-2025-22234

Description

The fix applied in CVE-2025-22228 inadvertently broke the timing attack mitigation implemented in `DaoAuthenticationProvider`.

Affected Spring Products and Versions

Spring Security:

- 5.7.16 only
- 5.8.18 only
- 6.0.16 only
- 6.1.14 only
- 6.2.10 only
- 6.3.8 only
- 6.4.4 only
- Older, unsupported versions are also affected

...

READ MORE

CVE-2025-22232: Spring Cloud Config Server May Not Use Vault Token Sent By Clients

MEDIUM | APRIL 07, 2025 | CVE-2025-22232

Description

Spring Cloud Config Server may not use Vault token sent by clients using a `X-CONFIG-TOKEN` header when making requests to Vault.

Your application may be affected by this if the following are true:

1. You have Spring Vault on the classpath of your Spring Cloud Config Server and
2. You are using the `X-CONFIG-TOKEN` header to send a Vault token to the Spring Cloud Config Server for the Config Server to use when making requests to Vault and
3. You are using the default Spring Vault `SessionManager` implementation `LifecycleAwareSessionManager` or a `SessionManager` implementation that persists the Vault token such as `SimpleSessionManager`...

READ MORE

CVE-2025-22223: Spring Security authorization bypass for method security annotations on parameterized types

MEDIUM | MARCH 19, 2025 | CVE-2025-22223

Description

Spring Security may not correctly locate method security annotations on parameterized types or methods. This may cause an authorization bypass.

Your application may be affected by this if the following are true:

1. You are using `@EnableMethodSecurity`, and
2. You have a method security annotation on a parameterized superclass, interface, or overridden method and no annotation on the target method

...

READ MORE

CVE-2025-22228: Spring Security BCryptPasswordEncoder does not enforce maximum password length

HIGH | MARCH 19, 2025 | CVE-2025-22228

Description

`BCryptPasswordEncoder.matches(CharSequence,String)` will incorrectly return `true` for passwords larger than 72 characters as long as the first 72 characters are the same.

Affected Spring Products and Versions

Spring Security:

- 5.7.0 - 5.7.15
- 5.8.0 - 5.8.17
- 6.0.0 - 6.0.15
- 6.1.0 - 6.1.13
- 6.2.0 - 6.2.9
- 6.3.0 - 6.3.7
- 6.4.0 - 6.4.3
- Older, unsupported versions are also affected

...

READ MORE

CVE-2024-38827: Spring Security Authorization Bypass for Case Sensitive Comparisons

MEDIUM | NOVEMBER 19, 2024 | CVE-2024-38827

Description

The usage of `String.toLowerCase()` and `String.toUpperCase()` has some `Locale` dependent exceptions that could potentially result in authorization rules not working properly.

Related to CVE-2024-38820

Affected Spring Products and Versions

Spring...

READ MORE

CVE-2024-38829: Spring LDAP Spring LDAP sensitive data exposure for case-sensitive comparisons

LOW | NOVEMBER 19, 2024 | CVE-2024-38829

Description

The usage of `String.toLowerCase()` and `String.toUpperCase()` has some `Locale` dependent exceptions that could potentially result in unintended columns from being queried

Related to CVE-2024-38820

Affected Spring Products and Versions

Spring LDAP:

- 2.4.0 - 2.4.3
- 3.0.0 - 3.0.9
- 3.1.0 - 3.1.7
- 3.2.0 - 3.2.7
- Older, unsupported versions are also affected

...

READ MORE

1 2 3 4 5 6 7 8 9 ... 16

Get ahead

VMware offers training and certification to turbo-charge your progress.

Learn more

Get support

Tanzu Spring offers support and binaries for OpenJDK™, Spring, and Apache Tomcat® in one simple subscription.

Learn more

Upcoming events

Check out all the upcoming events in the Spring community.

View all