spring by VMware Tanzu

Spring Security Advisories

RSS feed

CVE-2023-34034: WebFlux Security Bypass With Un-Prefixed Double Wildcard Pattern

HIGH | JULY 18, 2023 | CVE-2023-34034

Description

Using `"**"` as a pattern in Spring Security configuration for WebFlux creates a mismatch in pattern matching between Spring Security and Spring WebFlux, and the potential for a security bypass.

Affected Spring Products and Versions

Spring Security:

- 6.1.0 to 6.1.1
- 6.0.0 to 6.0.4
- 5.8.0 to 5.8.4
- 5.7.0 to 5.7.9
- 5.6.0 to 5.6.11

Mitigation

The following Spring Security versions contain fixes for this vulnerability:

- 6.1.2+
- 6.0.5+
- 5.8.5+
- 5.7.10+
- 5.6.12+

The above require Spring Framework versions:

- 6.0.11+
- 5.3.29+
- 5.2.25+

Credit

This vulnerability was disclosed responsibly by tkswifty and Ha1c9on.

References

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

Reporting a vulnerability

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

spring by VMware Tanzu

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

Why Spring
Generative AI
Microservices
Reactive
Event Driven
Cloud
Web Applications
Serverless
Batch

Learn
Quickstart
Guides
Courses
Get Certified

Projects

Resources
Blog
Release Calendar
Version Mappings
Release Highlights
Security Advisories

Community
Events
Authors

Enterprise
Long-term Support
Automated Upgrades
Governance and Compliance
Modern App Development

Thank You

Get the Spring newsletter

Stay connected with the Spring newsletter

SUBSCRIBE

spring by VMware Tanzu