Spring Security Advisories

All advisories

CVE-2024-38816: Path traversal vulnerability in functional web frameworks

HIGH | SEPTEMBER 12, 2024 | CVE-2024-38816

Description

Applications serving static resources through the functional web frameworks WebMvc.fn or WebFlux.fn are vulnerable to path traversal attacks. An attacker can craft malicious HTTP requests and obtain any file on the file system that is also accessible to the process in which the Spring application is running.

Specifically, an application is vulnerable when both of the following are true:

- the web application uses `RouterFunctions` to serve static resources
- resource handling is explicitly configured with a `FileSystemResource` location

However, malicious requests are blocked and rejected when any of the following is true:

- the Spring Security HTTP Firewall is in use
- the application runs on Tomcat or Jetty

Affected Spring Products and Versions

Spring Framework

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
5.3.x	5.3.40	Enterprise Support Only
6.0.x	6.0.24	Enterprise Support Only
6.1.x	6.1.13	OSS

No other mitigation steps are necessary.

Users of older, unsupported versions could enable Spring Security's Firewall in their application, or switch to using Tomcat or Jetty as a Web server because they reject such malicious requests.

Credit

The issue was identified and responsibly reported by Gabor Legrady.

References

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

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

Get the Spring newsletter

Stay connected with the Spring newsletter

SUBSCRIBE

spring by VMware Tanzu