VULNERABILITY BULLETINS

Patches Released for High-Severity Vulnerability (CVE-2024-38816) Affecting Spring Framework

TLP:WHITE

Sep 16, 2024

Spring Framework recently disseminated a security advisory to address a path traversal vulnerability, tracked as CVE-2024-38816, in functional web frameworks. Spring Framework is a popular Java-based open-source application framework that provides a comprehensive platform for building enterprise-level applications.

Applications serving static resources through the functional web frameworks WebMvc.fn or WebFlux.fn are vulnerable to path traversal attacks. Both are powerful tools for building web applications, and they operate as lightweight, functional programming models in which functions route and handle requests.

According to the Spring security advisory, an application is vulnerable when a web application uses RouterFunctions to serve static resources and resource handling is explicitly configured with a FileSystemResource location.

Successful exploitation will allow an adversary to 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.

Affected Spring Framework versions include:

- 5.3.0 - 5.3.39
- 6.0.0 - 6.0.23
- 6.1.0 - 6.1.12
- Older, unsupported versions are also affected

Health-ISAC provides this information for situational awareness and encourages users to upgrade affected Spring products to the appropriate fixed version.

Recommendations:

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and take the necessary actions to ensure appropriate security measures are implemented, including:

- Immediately apply available patches for affected versions.
- If an older version is being used, enable Spring Security's Firewall or,
- Switch to Tomcat or Jetty, as they inherently reject malicious requests
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

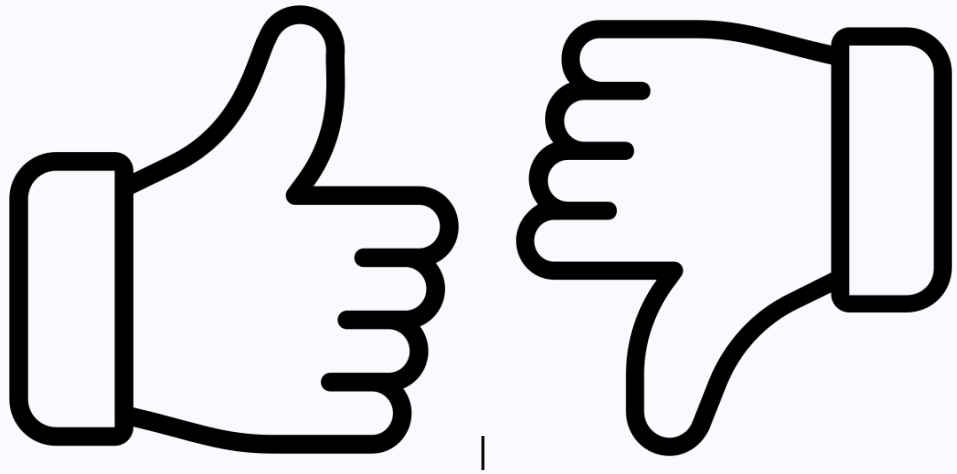
Reference(s)	Security Online, spring, spring, spring, HHS

Release Date
Sep 17, 2024 (UTC)

Alert ID c13401fd

View Alert

Share Feedback
was this helpful?



Tags CVE-2024-38816, Spring Framework

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**