VULNERABILITY BULLETINS

Spring Core on JDK9+ Vulnerable to Remote Code Execution

TLP:WHITE

Mar 31, 2022

On March 30, 2022, remediation guidance was shared for a vulnerability impacting Spring Core on JDK9+ due to a bypass for CVE-2010-1622. The new bug, dubbed SpringShell, or Spring4Shell, impacts Spring Core with Java Development Kit (JDK) versions greater than or equal to 9.0. In certain configurations, exploitation only requires an attacker to send a crafted POST request to a vulnerable system.

The Spring Core RCE bug was assigned CVE-2022-22965 on March 31, 2022.

A separate Spring Cloud bug was assigned CVE-2022-22963 on March 29, 2022.

In JDK9+ a remote attacker can obtain the AccessLogValve object and malicious field values through the parameter binding function.

The exploit is relatively easy to execute in a similar manner to Log4Shell, hence the names SpringShell, or Spring4Shell. The public exploit available has been confirmed valid in a demo environment.

There is no official patch available for the vulnerability.

Mitigation:

Implement WAF protection rule filtering for strings such as class.*, Class.*, *.class, and *.Class consistent with expected traffic of authorized services.

Remediation:

In Spring Framework, DataBinder has functionality to disallow defined patterns. Creation of a ControllerAdvice component with dangerous patterns added to the deny list may be an effective strategy.

Additional context, including an example snippet is available from praetorian.

Reference(s)	spring, spring, praetorian, Cyber Kendra, Security Boulevard, Flashpoint

Release Date
Mar 31, 2022

Alert ID bb60f0a4

View Alert

Tags JDK9+, Spring Core

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

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

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

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.