

ALERT





Spring Releases Security Updates Addressing "Spring4Shell" and Spring Cloud Function Vulnerabilities

Last Revised: April 01, 2022



Spring by VMWare has released Spring Cloud Function versions 3.1.7 and 3.2.3 to address remote code execution (RCE) vulnerability CVE-2022-22963 as well as Spring Framework versions 5.3.18 and 5.2.20 to address RCE vulnerability CVE-2022-22965, known as "Spring4Shell." A remote attacker could exploit these vulnerabilities to take control of an affected system.

According to VMware, the Spring4Shell vulnerability bypasses the patch for [CVE-2010-1622](#), causing CVE-2010-1622 to become exploitable again. The bypass of the patch can occur because Java Development Kit (JDK) versions 9 and later provide two sandbox restriction methods, providing a path to exploit CVE-2010-1622 (JDK versions before 9 only provide one sandbox restriction method).

CISA encourages users and administrators to immediately apply the necessary updates in the Spring Blog posts that provide the [Spring Cloud Function updates addressing CVE-2022-22963](#)  and the [Spring Framework updates addressing CVE-2022-22965](#) . CISA also recommends reviewing VMWare Tanzu Vulnerability Report [CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+](#)  and CERT Coordination Center (CERT/CC) Vulnerability Note [VU #970766](#)  for more information.

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.



Please share your thoughts

We recently updated our anonymous [product survey](#); we'd welcome your feedback.