Neat Statement on the Spring4Shell Exploit

Last updated on April 21, 2022

CVE-2022-22965

At the end of March 2022, three critical vulnerabilities in the Java Spring Framework were published, including a remote code execution (RCE) vulnerability called Spring4Shell or SpringShell.

The **critical severity flaw**, assigned the identifier CVE-2022-22965 (CVSS score: 9.8) and dubbed "Spring4Shell", impacts Spring model–view–controller (MVC) and Spring WebFlux applications running on Java Development Kit 9 and later.

What is Spring4Shell?

Spring4Shell is a critical vulnerability in the Spring Framework, an open source platform for Java-based application development. Due to its popular use with developers and software engineers, many applications are potentially affected. The Spring Framework enables developers to build Java applications faster and more conveniently while reducing configuration complexity and costs.

What is the Impact of Spring4Shell?

The vulnerability could allow malicious actors to achieve remote code execution in Spring Core applications under non-default circumstances, granting the attackers full control over the compromised devices. Because Spring4Shell exposes an application to remote code execution, an attacker can possibly access all website internal data, including any connected database. It may also allow an attacker to access additional internal resources to gain more permissions or to make their way to other parts of an internal network.

What is Neat's Exposure?

Important note: Neat does not use the Spring framework and therefore Neat devices are not affected by the Spring4Shell vulnerability. Devices include Neat Bar, Neat Pad, Neat Bar Pro, Neat Board, and Neat Frame.

As this is an evolving incident, our team is continuing to investigate and validate additional information about this vulnerability and its impact, including assessing the risk to our third-party

vendors that we use for client management and sales processes.If you have any further questions or security concerns, please send an email to *security@neat.no* or log a ticket with our customer support.

Additional References:

- VMWare “CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+”
- VMWare "CVE-2022-22963: Remote Code Execution in Spring Cloud Function by Malicious Spring Expression
- Spring “Spring Framework RCE, Early Announcement”
- CISA “Spring Releases Security Updates Addressing "Spring4Shell" and Spring Cloud Function Vulnerabilities”
- CVE.org “2022-22965”