Warning of dangerous Spring4Shell vulnerability, there are signs of scanning and exploiting

Spring has just released an urgent update to patch the Spring4Shell remote code execution zero-day vulnerability. Information about this vulnerability was leaked on the internet before the patch was released.

Soon after, a guide to exploiting the Spring4Shell vulnerability in the Spring Framework was posted on GitHub and deleted. But the internet was an open world, so that exploit was quickly re-shared elsewhere and tested and confirmed by security researchers as a standard Spring4Shell-only exploit.

The Spring4Shell vulnerability exists in Spring Core, a core component of the Spring Framework open source code. Currently, Spring Framework is commonly used in web applications. It is estimated that about 50% of web applications written in Java use Spring Core. According to the assessment, Sping4Shell is more dangerous than the Log4Shell vulnerability, one of the most dangerous vulnerabilities of the decade that was discovered at the end of 2021.

According to the Cybersecurity Monitoring Center, there have been groups of hackers that have scanned and tested Spring4Shell on some technology systems of agencies and organizations.

To fix the vulnerability, IT admins need to update to the following versions:

1. Spring Framework 5.3.18 and Spring Framework 5.2.20.
2. Spring Boot 2.5.12.
3. Spring Boot 2.6.6 (to be released soon).

The Spring4Shell vulnerability is particularly dangerous because developers often use sample code for their applications. Therefore, many applications are at risk of being attacked online.

Admins need to prioritize deploying updates as soon as possible. The reason is because hackers are actively exploiting new vulnerabilities.