Spring4Shell：Java 架構中發現新的零日 RCE 漏洞

2022 年 3 月 31 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

賽門鐵克產品將防護對 Spring4Shell 漏洞的利用企圖。

3 月 30 日，在發布修正程式之前，Spring Core Java 架構中的一個零日漏洞可能允許對易受攻擊的應用程序進行未經身份驗證的遠端程式碼執行 (RCE)。它被稱為 Spring4Shell。

賽門鐵克產品能否防護此攻擊企圖？

是的，賽門鐵克產品將通過以下檢測來防範利用嘗試：

基於網路特徵

- Web Attack: Spring Core Spring4Shell Activity 2
- Audit: Web Attack: Spring Core Spring4Shell Activity

Spring4Shell 有可用的修正程式嗎？

Spring 現在已經發布了 Spring Framework 5.3.18 和 5.2.20，據說修復了這個漏洞。相依於 Spring Framework 5.3.18 的 Spring Boot 2.6.6 和 2.5.12 也已經發布。在發布更新之前，Praetorian 的研究人員還公布臨時修復步驟。Spring 還在其部落格中發布建議的解決方法。

該漏洞的 CVE 報告也在今天下午發布，命名為 CVE-2022-22965，評估為“高嚴重性”。

這個漏洞有多嚴重？

人們似乎對 Spring4Shell 的潛在嚴重性感到疑惑。雖然最初報告說 JDK 版本大於或等於 9.0 的所有 Spring Core 版本都容易受到它的攻擊，但研究人員隨後確定 Spring Core 似乎必須以某種方式設定才較易受到攻擊。

在其漏洞報告中，Spring 本身表示，要使“特定漏洞利用”起作用，應用程式必須滿足以下先決條件：

- JDK 9 或更高版本
- Apache Tomcat 作為 Servlet 容器
- 封裝為 WAR
- spring-webmvc 或 spring-webflux 有相依性

該公告中寫道：“如果應用程式被部署為 Spring Boot 可執行 jar，即預設值，它就不容易受到漏洞利用”。不過，它也確實表示“該漏洞的性質更為普遍，可能還有其他方法可以利用它。”

鑑於這些先決條件，尚不清楚有多少 Spring Core Java 架構實例可能容易受到此錯誤影響。

Spring4Shell 是否已廣泛的被主動利用？

於發布修正程式之前，Spring4Shell 的概念驗證漏洞利用程式碼在被發現後不久後就在 GitHub 上披露。雖然該程式碼被迅速刪除，但在確認該漏洞的幾位安全研究人員下載之前。它還在各種平台上被轉發，這意味著它可供大眾利用，包括惡意行為者。據報導，Spring4Shell 已被發現在攻擊事件中被主動利用。

什麼是 Spring4Shell ？

Spring4Shell 是 Spring Core 中的一個 bug，Spring Core 是一個普遍的應用程式架構，它允許軟體開發人員快速輕鬆地開發具有企業級功能的 Java 應用程序。然後可以將這些應用程序部署在伺服器上，例如：Apache Tomcat，該獨立封裝具有所有相依性的程式碼。

該漏洞允許未經身份驗證的攻擊者在易受攻擊的系統上執行任意程式碼。

在周四（3 月 31 日）發布的部落格中，Spring 透露，週二 AntGroup FG 的研究人員向 VMware（擁有 Spring）報告了 Spring4Shell 漏洞，該團隊打算在周四發布針對該漏洞的緊急修正程式，但漏洞的一部分詳細訊息該於週三在網上被洩露。

Spring4Shell 是否與 CVE-2022-22963 相關？

不，CVE-2022-22963 是 Spring Cloud Function 中的另一個錯誤，它是一個獨立於 Spring Core 的 Java 程式庫。3 月 29 日發布了有關此錯誤的公告，並提供修正程式。

這個新的 bug 和 Log4Shell 一樣嚴重嗎？

雖然該漏洞的命名似乎受到了 2021 年 12 月發現的 Log4Shell 漏洞的啟發，但尚不清楚該漏洞的影響是否會如此顯著。

在獲得任何新的相關訊息時，我們將會更新此部落格。

防護

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/spring4shell-rce-vuln-java
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2022/04

關於作者

威脅獵手團隊
賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588