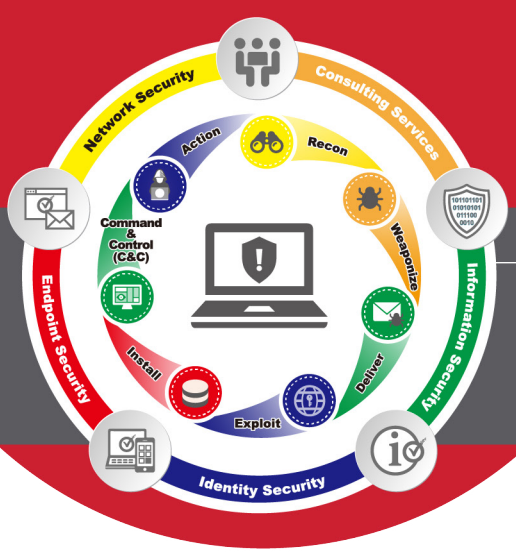


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

Apache ActiveMQ漏洞(CVE-2023-46604)仍被大肆開採濫用

2024 年 2 月 13 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

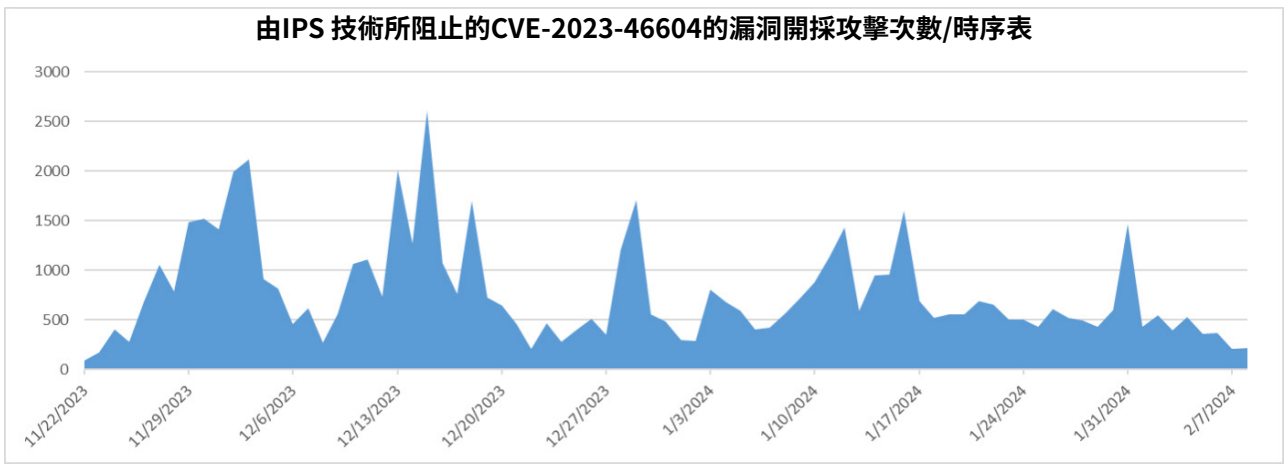
Apache ActiveMQ 是一個用 Java 撰寫的開源訊息代理程式。可促進不同的企業級應用程式、服務和系統之間的訊息傳遞提供高可用性、可擴展性、可靠性、性能和安全性。

CVE-2023-46604 是一個存在 Apache ActiveMQ 的嚴重等級 (CVSS 風險評分：10) 遠端程式碼執行 (REC) 漏洞。如果被成功開採濫用，未經認證的遠端攻擊者，可在有機可趁的系統上執行任意 shell 命令。由於該漏洞很容易被開採濫用，攻擊者可以很快將其整合到他們攻擊手法中，以入侵企業環境並傳播各種惡意軟體有效籌載。

賽門鐵克已觀察到攻擊者成功開採濫用該漏洞後，傳遞以下惡意軟體的有效載荷：

- Linux 惡意軟體讓攻擊者操控遭入侵的 Linux 機器。
- 惡意挖礦程式，可在遭入侵的 Linux 和 Windows 機器上暗中執行挖礦程式。
- 反向 shell 有效籌載，可以獲取遭入侵機器的後門存取權限。
- Kinsing 惡意軟體，執行挖礦程式，並試圖將自身傳播到環境中的其他系統。
- Paradise、TellYouThePass 和 HelloKitty 等多種勒索軟體變來加密系統中的檔案，破壞其可用性。
- Shellbot 用於入侵伺服器，然後發動 DDoS 攻擊並傳遞惡意挖礦程式。

賽門鐵克的網路層防護技術：入侵預防禦系統 (IPS) 可有效阻止這些漏洞利用嘗試，防止系統受到感染／入侵。攻擊在初始階段就會被阻止，進而確保沒有惡意有效籌載駭入系統。迄今為止，IPS 技術已阻止超過 60K 次意圖開採濫用該漏洞的網路攻擊。



賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Attack: Apache ActiveMQ RCE CVE-2023-46604
- System Infected: Bad Reputation Process Request
- Web Attack: Malicious Java Payload Download

基於行為偵測技術(SONAR)的防護：

- SONAR.Cryptolocker!g75
- SONAR.MalTraffic!gen1
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g253
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Malscript!g1
- Ransom.HelloKitty
- Ransom.Tellyouthepass
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- Ransom.Paradise
- Linux.Kaiten
- Scr.Malcode!gen
- IRC.Backdoor.Trojan

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.C

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security其出廠就內建的系統鎖定政策，可以保護底層的作業系統免受此漏洞的侵擾。DCS 的網路規則政策可設定為，將 ActiveMQ 應用程式限制為受信任的用戶端。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

欲瞭解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片）軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。