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

IPS(入侵防禦系統)阻止了數百萬次Log4j攻擊

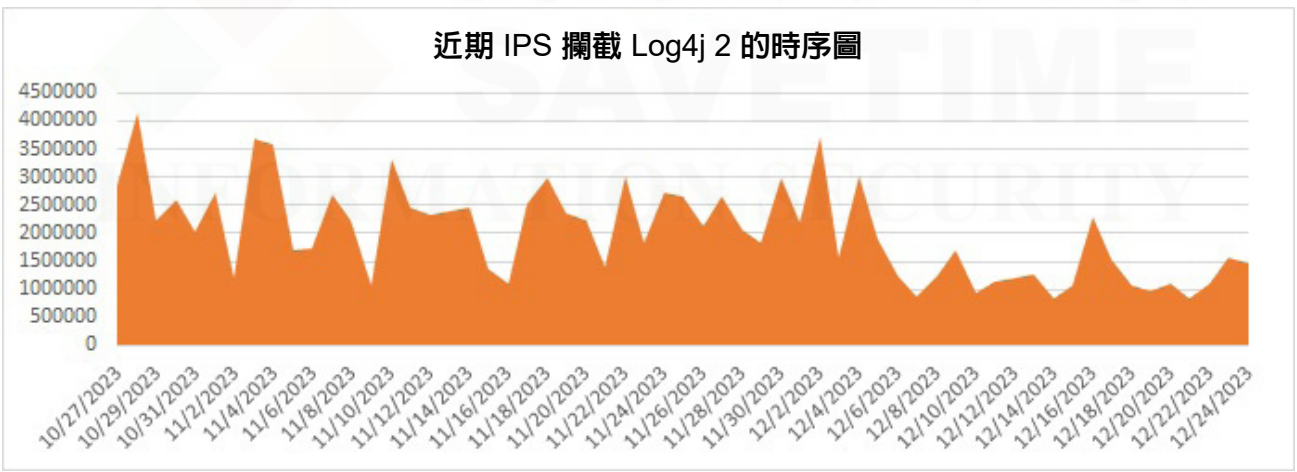
2023 年 12 月 26 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

眾所周知，有許多漏洞早已被修補，但仍被世界各地的駭客組織和個體戶大肆開採濫用。雖然大多數漏洞在被披露的當年影響最大、破壞性最強，但有些漏洞在多年後仍然非常有效，例如：Log4j RCE CVE-2021-44228。

該漏洞於 2021 年被披露，被廣泛稱為『Log4Shell』，是 Apache Log4j 2 函式庫 (一種常見基於 Java 的日誌應用系統) 中出現一個嚴重等級的安全性漏洞。這個漏洞能導致應用程式被提權，讓遠端攻擊者得以有足夠的權限來執行任意程式碼，對尚未完全修補漏洞採用 Log4j 的日誌系統所有應用系統或程式構成重大風險。

賽門鐵克每天都能監控到世界各地的威脅行動者試圖開採濫用這個漏洞，您可以從下面 IPS(入侵防禦系統) 遙測圖表中看到這一點 (請注意，賽門鐵克將這些攻擊攔截為『Log4j2』)。雖然我們針對這一漏洞提供其他防護機制，包括標準的防毒技術和基於安全政策強制的 DCS 政策，但由於攻擊的性質 (網路層，無檔案行威脅) 我們的 IPS 技術能夠更好地防禦這一漏洞，本文章僅介紹我們基於網路的保護措施--IPS。



網路有許多探討關於陳年老舊或已經進行修補的漏洞持續遭受惡意行動者開採濫用資訊。其中一些主要原因如下：

- **老舊系統**：組織繼續使用老舊的系統是個棘手問題，這些系統難以升級，儘管有可用的修補程式，但仍暴露在風險中。
- **資訊落差**：並非每個人都能及時瞭解情況或採取行動。漏洞意識和進行修補之間的落差使攻擊者得開採濫用已知的弱點。
- **資源不足**：巧婦難為無米之炊 (尤其是中小型企業組織) 資源不足導致無法定期更新，使其容易遭開採濫用。
- **料敵如神**：攻擊者戰略性地瞄準眾所周知的漏洞，看準並非所有系統都會及時進行修補的心態。
- **拿捏平衡**：系統管理員在安全性和運行穩定性之間取捨掙扎，往往會延遲進行修補以避免重新開機或藍+底字的中斷。
- **人類的惰性**：拒絕改變是常見的人格特質，這也是為什麼儘管存在已知風險，但陳年漏洞仍持續被開採濫用的主因。

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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

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: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j2 RCE CVE-2021-44228 4

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。

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**。