SEP第一時間有效攔截漏洞開採利用～程式語言 PHP 存在PHP-CGI引數注入(Argument Injection)漏洞：CVE-2024-4577

2024 年 7 月 2 日發布

程式語言 PHP 存在 PHP-CGI 引數注入 (Argument Injection) 漏洞：CVE-2024-4577， 正在被大肆開採濫用

PHP 是一種通用伺服器指令碼語言，是製作動態互動式網頁的強大腳本工具。CVE-2024-4577 是一個高嚴重性等級 (CVSS風險評分：9.8) 的參數注入漏洞，當 PHP 以 CGI 模式執行時會受到影響。該漏洞是由於在 Windows 上執行 PHP 時失誤造成的，特別是與程式碼轉換 Best-Fit 功能相關。如成功開採濫用此漏洞，未經認證的攻擊者可在受影響的 PHP 伺服器上執行任意程式碼，導致系統被完全入侵及隨後的惡意軟體傳遞。由於 PHP 是一種廣泛使用的指令碼語言，攻擊者很快就開始利用這一漏洞入侵網路並部署不同類型的惡意軟體有效酬載。有證據顯示該漏洞被大肆開採濫用後，美國網路安全暨基礎設施安全局 (CISA) 最近將該漏洞新增到「已知成功利用漏洞列表 (the Known Exploited Vulnerabilities Catalog-KEV)」目錄中。

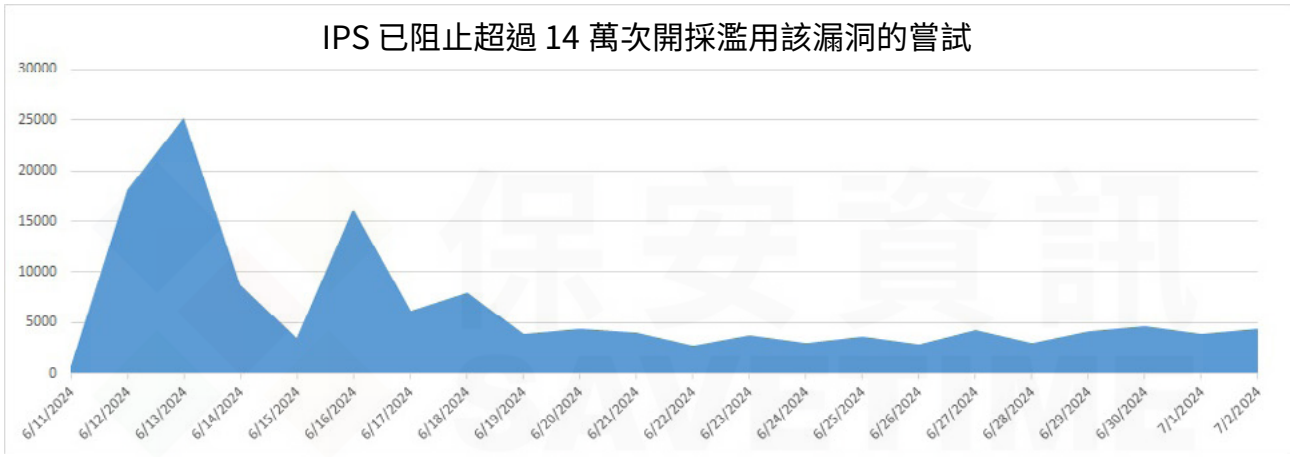
觀察到的惡意軟體有效酬載

賽門鐵克已觀察到威脅行為者利用此漏洞後發送的以下惡意軟體有效酬載：

- TellYouThePass 勒索軟體，它會加密系統中的檔案，使其無法使用
- Web shell 有效酬載，用於獲取受攻擊電腦的後門存取權限
- 流行的威脅模擬工具 CobaltStrike
- 在被入侵的 Windows 機器上進行挖礦劫持
- Mirai 殭屍網路，主要在劫持物聯網 (IoT) 設備並將其接管變成遠端控制的『機器人』

賽門鐵克的防護技術集

賽門鐵克端點防護上的網路層防護技術：入侵防護系統 (IPS) 與賽門鐵克其他多層次防護技術的協同防護架構，可阻止這些漏洞利用嘗試，防止系統受到感染／破壞。IPS 在初始階段就能阻止攻擊，進而確保不會向系統注入惡意有效酬載。迄今為止，IPS 已阻止超過 14 萬次開採濫用該漏洞的嘗試。



研究人員發現 PHP 存在引數注入 (Argument Injection) 漏洞 (CVE-2024-4577)，未經身分鑑別之遠端攻擊者，可透過特定字元序列繞過舊有 CVE-2012-1823 弱點修補後之保護，並透過引數注入等攻擊於遠端 PHP 伺服器上執行任意程式碼，請儘速確認並進行修補。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspScript!g7
- SONAR.SuspLaunch!g18
- SONAR.Downloader!gen2
- SONAR.Trafic1.RGC!g10
- SONAR.Dropper

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- Ransom.Zombie
- Trojan Horse
- Trojan.Gen.MBT
- Hacktool.Mimikatz
- WS.Malware.1
- Backdoor.Doublepulsar
- IRC.Backdoor.Trojan
- Backdoor.Cobalt
- Linux.Trojan

基於機器學習的防禦技術：

- Heur.AdvML.B!100
- Heur.AdvML.B!200

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：

- Web Attack: PHP-CGI Argument Injection Vulnerability CVE-2024-4577
- Web Attack: Malicious Payload Download 21

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完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
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。
賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。
欲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**。