



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

2026 年上半年賽門鐵克 IPS 阻擋的前四大攻擊手法

2026 年 8 月 3 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

漏洞是指軟體、硬體或設定中的弱點，攻擊者可藉此利用，使系統產生非預期行為。對攻擊者而言，漏洞極少是最終目標—它只是起點；是攻擊者用以入侵企業環境，並進一步轉向更具破壞性目標的初始立足點。一旦成功利用漏洞，攻擊者通常會利用該存取權限來：

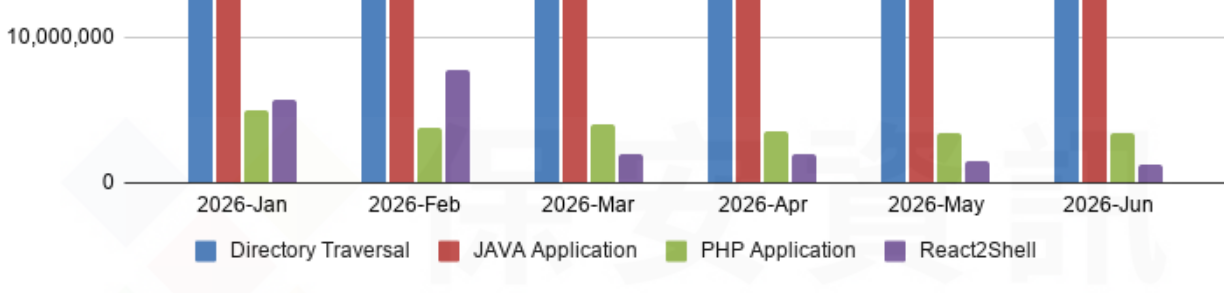
- 部署 WebShell 或後門程式，以維持對受感染系統的持久性遠端存取。
- 竊取敏感資料—包括憑證、智慧財產權、客戶紀錄或設定檔。
- 部署勒索軟體以加密關鍵系統，並向組織勒索贖金。
- 劫持運算資源用於加密貨幣挖礦，導致系統效能下降並推高成本。
- 在網路中進行橫向移動，以存取更高價值的系統與帳戶。
- 建立指揮與控制 (C2) 通道，以接收進一步指示或部署其他工具。
- 蒐集憑證以提升權限，並擴大入侵範圍。

這些結果無一例外都取決於同一個先決條件：漏洞利用必須先成功執行。這正是網路防護機制發揮作用的時機。

賽門鐵克入侵防禦系統 (IPS) 會將網路流量與持續更新的、基於漏洞的特徵碼資料庫進行比對，在漏洞利用有效載荷尚未抵達終端裝置或在終端裝置上執行之前，便在傳輸過程中阻擋攻擊流量。這使得 IPS 處於攻擊鏈的 感染前 階段：即攻擊者仍在嘗試取得上述所述的初始立足點，但尚未成功的階段。這正是 IPS 成為預防性資安基石的原因—它在感染、加密或資料外洩成為可能之前，便已將攻擊扼殺於萌芽狀態。

在 2026 年 1 月至 6 月期間，有四類攻擊手法主導了賽門鐵克 IPS 在網路層攔截的內容，根據我們的全球遙測數據，這些攻擊共計佔了約 **2.87 億次攔截事件**。其中三類是已存在數十年的技術類別，至今仍大規模地發揮作用；第四類則是在六個月前還不存在的。

Top 4 exploitations attempts blocked by Symantec IPS technology



2026 年上半年，賽門鐵克 IPS 阻擋的前四大攻擊嘗試類別。

資料來源：賽門鐵克 IPS 遠端監測資料，2026 年 1 月至 6 月。

這份排名僅揭示了部分真相。在整個觀察期間內，若以月對月比較來看，目錄遍歷、Java 漏洞利用及 PHP 漏洞利用的狀況基本上維持穩定—既未出現下降趨勢，也無季節性波動，更未顯示潛在漏洞風險正在消除的跡象。而 React2Shell 的表現則與它們截然不同。

#1—目錄遍歷

目錄遍歷（亦稱路徑遍歷）是利用 Web 應用程式對使用者或客戶端請求所傳入的檔案路徑輸入驗證不足的漏洞。攻擊者透過注入諸如：/、URL 編碼等價形式 (%2e%2e%2f) 或絕對路徑等字串，可繞過應用程式原本應受限的目錄範圍，遍歷其檔案處理邏輯，從而存取檔案系統中其他位置的任意檔案。在最簡單的情況下，這會導致敏感檔案、應用程式設定、憑證或原始碼外洩。當同一漏洞允許寫入而不僅限讀取時—例如：上傳端點未能對目標路徑進行淨化處理—攻擊者便可透過在 Web 根目錄中植入惡意檔案，直接升級為遠端程式碼執行。

這項技術已有約三十年的文獻記載，且至今仍未過時。它年復一年地出現在美國網路安全與基礎設施安全局 (CISA) 的「已知遭利用漏洞」(KEV) 目錄中，通常在漏洞披露後數日內，便會有公開的概念驗證攻擊程式問世：

- **CVE-2021-41773—Apache HTTP 伺服器 (CVSS 9.8)**：Apache 2.4.49 中的路徑正規化漏洞。當受影響的路徑被映射至 CGI 處理程式時，檔案洩露將直接升級為遠端程式碼執行。儘管修補程式已發布五年，針對未修補實例的攻擊嘗試仍持續發生。
- **CVE-2025-2749—Kentico Xperience CMS (CVSS 7.2)**：Staging Sync Server 中的路徑遍歷漏洞，該服務會將上傳的檔案寫入路徑相對位置。
- **CVE-2026-48282—Adobe ColdFusion (CVSS 10.0, CWE-22)**：遠端開發服務 (RDS) 的 FILEIO 處理程式中存在未經身份驗證的路徑遍歷漏洞。系統在處理使用者提供的路徑字串時，未進行規範化處理或根目錄驗證，導致可執行任意檔案寫入操作；且透過將 CFML 寫入 Web 根目錄，可使攻擊者以 ColdFusion 服務帳戶身分進行未經認證的程式碼執行。Adobe 已於 2026 年 6 月 30 日發布修補程式；在修補程式分析完成後數日內，攻擊者便開始利用此漏洞發動攻擊，而 CISA 則於 2026 年 7 月 7 日將此漏洞新增至 KEV 清單中。

#2—Java 應用程式／框架漏洞利用

Java 應用程式與框架的漏洞利用涵蓋了一系列不同的根本原因，但最終結果都相同：由攻擊者控制的程式碼在 JVM 內執行。最常見的促成因素包括：

- **不安全的反序列化**—應用程式在未驗證類型或內容的情況下，對攻擊者提供的 Java 物件進行反序列化，導致應用程式自身函式庫中已存在的「小工具鏈」觸發任意方法呼叫。
- **表達式語言注入**—本應被視為資料處理的用戶輸入，卻被框架本身當作可執行程式碼進行評估。
- **無限制檔案上傳**至應用程式伺服器將執行的位置，使攻擊者能直接將 WebShell 或編譯後的類別檔案植入執行環境中。

由於這些是底層平台或框架本身的弱點，而非任何單一應用程式的業務邏輯問題，因此無論它們在該框架上建構了什麼服務，單一漏洞便可能影響所有運行該框架或設備的組織。這使得廣泛部署的通用 Java 平台成為特別吸引人且反覆遭攻擊的目標—攻擊者最常鎖定的目標包括 Apache Struts、Apache Tomcat、Oracle WebLogic Server、Spring Framework、Atlassian Confluence 與 Jira、Apache Solr、Apache OFBiz 以及 Jenkins—因為只要針對其中任何一個平台開發出有效的攻擊程式碼，就能直接套用到所有運行相同平台的組織。

暴露於不可信任網路中的企業級 Java 中介軟體，仍是說明此類暴露狀況會持續多久的最明顯例子：

- **CVE-2020-14882—Oracle WebLogic Server (CVSS 9.8)**：WebLogic 控制台存在一項認證繞過漏洞，允許未經認證的攻擊者透過發送單一經過特殊設計的 HTTP 請求，完全掌控主機。時隔六年，根據我們的遙測數據，這仍是 WebLogic 中最常被嘗試利用的漏洞之一。
- **CVE-2024-21182—Oracle WebLogic Server (CVSS 7.5)**：一項未具體說明的漏洞，允許透過 T3 或 IIOP 取得網路存取權限的未經認證攻擊者，入侵該伺服器。Oracle 已在 2024 年 7 月的「關鍵修補程式更新」中修復此漏洞；CISA 則於 2026 年 6 月 1 日—近兩年之後—將其納入 KEV 清單，並設定為期四天的聯邦層級補救期限。修補程式發布與確認大規模攻擊之間的時間差正是關鍵所在：儘管修補程式已存在兩年，但系統漏洞仍持續存在。

#3 — PHP 應用程式／框架的漏洞利用

PHP 驅動了網際網路上大量內容管理系統與客製化商業應用程式，而此類攻擊主要仰賴一種特別直接的技術：一旦攻擊者能將 .php 檔案放置於任何可透過網頁存取的目錄中，當該檔案被請求時，網頁伺服器便會立即將其作為腳本執行—無需額外的編譯、注入或進程劫持步驟。這使得不受限制的檔案上傳端點，成為取得持久性 WebShell 的極其可靠途徑。

第二項主要攻擊途徑是 PHP 物件注入。許多 PHP 應用程式依賴原生序列化功能，當不可信的輸入傳遞至 unserialize() 函式時，攻擊者便能構建一個物件，其魔術方法會在物件反序列化的瞬間執行攻擊者自選的程式碼—這與導致 Java 中不安全反序列化的弱點屬同一類別，且是透過 PHP 自身的物件模型實現的。第三種途徑較為狹窄，即針對 PHP CGI 處理程式的參數注入，此處會將經過精心設計的查詢字串作為命令列參數傳遞給 PHP 二進位檔。

由於 PHP 應用程式部署範圍極廣，且經常直接對外連線至網際網路，因此熱門內容管理系統 (CMS) 或框架中的單一漏洞，便可能被利用來攻擊數百萬個安裝實例。這使得眾所周知的 PHP 平台—例如：WordPress 核心及其外掛／佈景主題生態系統、Drupal、Joomla、Magento、Laravel、phpMyAdmin、Roundcube、ThinkPHP 以及 CodeIgniter—屢屢成為攻擊者的首選目標，原因正是因為單一有效的漏洞利用程式便能觸及大量獨立且直接對外公開的安裝環境。

- **CVE-2026-48939—Joomla 的 iCagenda 擴充套件 (CVSS 3.1：9.8 / CVSS 4.0：10.0)**：活動提交表單僅在檢視層執行其「僅限已註冊用戶」的存取限制，卻未在控制層執行，因此直接向註冊處理程序發送 POST 請求即可完全繞過此限制。上傳的附件會以原始副檔名寫入 Web 根目錄，且未進行白名單篩選、MIME 檢查或內容驗證—一個 .php 檔案會被放置於可透過 Web 存取的文件目錄中，並在首次請求時被執行。此漏洞在 2026 年 6 月 15 日修補程式發布前已遭實際利用；於 2026 年 7 月 10 日新增至 KEV。
- **CVE-2025-49113—Roundcube Webmail (CVSS 9.9)**：設定模組的檔案上傳處理機制中存在 PHP 物件反序列化漏洞，允許經認證的攻擊者實現遠端程式碼執行。
- **CVE-2024-4577—Windows 上的 PHP-CGI (CVSS 9.8)**：一項參數注入漏洞，透過 Windows 的「最佳匹配」字元轉換機制繞過針對 CVE-2012-1823 的修補措施，允許未經認證的遠端程式碼執行。自披露以來，此漏洞已被一般網路犯罪者及勒索軟體營運者廣泛利用。

第 4 名—React2Shell

躋身前四名的最新成員是 CVE-2025-55182，這是 Meta 的 React Server Components (RSC) 中一項被安全業界稱為 React2Shell 的嚴重漏洞。該漏洞由 Meta 與 Vercel 於 2025 年 12 月 3 日公開披露，其 CVSS v3.1 評分為 10.0 (CVSS v4：9.3)—這是最高評級，專用於那些無需認證、無需使用者互動，且能直接導致遠端程式碼執行的漏洞。

根本原因在於 RSC 的「Flight」協定中，對序列化資料的處理存在安全漏洞；該協定是 React 用於在伺服器與客戶端之間傳遞元件樹及惡意的機制。攻擊者向運行 React Server Components 的應用程式發送單一經過精心設計且包含惡意有效載荷的 POST 請求，後端在未進行充分驗證的情況下處理該請求，進而執行由攻擊者控制的程式碼。預設配置會受到影響：使用 create-next-app 建置並部署至生產環境的標準應用程式，即使開發人員完全未修改程式碼，仍可能遭到利用。

與上述三類不同，React2Shell 僅是一個 CVE 編號，而非某種技術類別—而它僅憑阻擋量就躋身前四名。這就是整個故事。漏洞披露後數小時內便出現攻擊行為，而 CISA 則在約 48 小時後 (2025 年 12 月 5 日) 將此漏洞納入其 KEV 目錄。此漏洞威脅活動範圍廣泛，從機會主義式的加密貨幣挖礦，到疑似與國家有關聯的間諜行動，不一而足。

我們的遙測數據隨後顯示出其他三類從未出現過的現象：下降趨勢。被攔截的事件量在 2026 年 2 月達到高峰，約為 760 萬起；3 月降至約 180 萬起；到了 6 月則進一步下滑至約 110 萬起—四個月內較高峰期的暴跌 85%。這正是大規模機會主義式攻擊的典型曲線：隨著修補程式普及率提升，以及自動化掃描轉向更具潛力的目標，此類攻擊最終會自行消退。

這種衰退現象正是好消息，而我們值得仔細釐清其發生原因：該漏洞是可以修補的，修補程式也已發布，且有足夠多的網路使用者安裝了修補程式，以致於持續進行掃描已無利可圖。

前四名的背後規律

若不拘泥於排名，其背後的規律便一目了然：上半年有三個類別表現持平，而其中一個則呈現下滑趨勢。

這三項漏洞則構成了這幅圖景的其餘部分。目錄遍歷、Java 框架漏洞利用以及 PHP 檔案上傳濫用，數十年來一直是攻擊者的常用手段，而它們在我們的遠程監測數據中位居榜首，原因其實並不光鮮：它們至今依然有效。這些存在漏洞的軟體直接對外連線、廣泛部署，且在修補程式發布後很長一段時間內仍未獲修補。CVE-2024-21182 於 2026 年 6 月被收錄至 KEV 目錄，該漏洞針對的是 Oracle 於 2024 年 7 月發布的修補程式。CVE-2021-41773 在補救措施推出五年後，仍持續觸發阻擋事件。修補程式的可用性與實際部署並非同一回事，而攻擊者正是利用這道鴻溝來規劃攻擊目標。這道鴻溝的具體體現，便是長達六個月的攻擊量數據。

React2Shell 也展示了前端可能發生的相反失敗模式。從漏洞曝光到大規模利用，僅耗時數小時，而非數月。無論修補週期如何嚴謹，都無法達到這種速度。在這段時間內，網路層偵測並非修補措施的輔助手段；它是當下唯一可行的防禦措施。

這正是將 IPS 視為主要預防性控制措施而非次要措施的原因。簽名檔能在數小時內全球部署，且由於其針對的是攻擊技術而非特定供應商的建置版本，因此針對某類攻擊的防護範圍，往往能在該類型的下一項 CVE 公開披露前，便已將其阻擋。對於無法隨需修補的系統—例如：舊有的業務線應用程式、等待供應商修正的設備，以及仍承載產線負載的已終止支援平台—入侵防禦系統 (IPS) 往往是阻隔已暴露漏洞與實際入侵之間唯一的屏障。

賽門鐵克的 IPS 防護範圍已針對所有四個類別完成部署且處於最新狀態。我們建議確認桌面電腦和伺服器均已啟用 IPS，並確認 Windows 端點已啟用「瀏覽器防護」。

賽門鐵克可保護您免受以下威脅的侵害，這些威脅的識別資訊如下：

基於網路的威脅 — 目錄遍歷

- [32494] Attack: Generic Directory Traversal 2
- [33453] Web Attack: Generic Directory Traversal 5
- [30413] Web Attack: Passwd File Download Attempt

基於網路 — Java 應用程式／框架漏洞利用

- [31490] Web Attack: Malicious Java Payload Upload 2
- [31865] Web Attack: Malicious Java Payload Upload 5
- [32680] Web Attack: Malicious Java Payload Upload 9

基於網路 — PHP 應用程式／框架漏洞利用

- [34889] Web Attack: PHP Shell Upload 15
- [34704] Web Attack: PHP CGI Argument Injection CVE-2024-4577

基於網路 — React2Shell

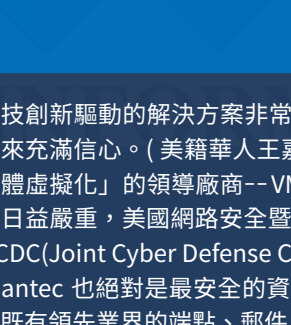
- [35256] Web Attack: Meta React Server Components CVE-2025-55182
- [35300] Web Attack: Meta React Server Components CVE-2025-55182 2
- [35273] Web Attack: Malicious Payload Upload 40

欲深入瞭解如何在桌面電腦和伺服器上啟用 IPS，[請點擊此處](#)。

欲深入瞭解如何在 Windows 桌面電腦上啟用 IPS 瀏覽器防護，[請點擊此處](#)。

尚未安裝 SEP？不妨嘗試使用 [賽門鐵克瀏覽器防護](#) 來保護您的瀏覽器。

原廠網址：https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-top-four-exploitation-techniques-blocked-by-symantec-ips-h1-2026
本文係由保安資訊有限公司專業細心整理後提供。如有遺漏、更新或異動均以上Symantec原廠公告為準，請知悉。



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構產生的頭版文章中，而且在全球前兩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組合，也顯示大型企業顧客對博通中的新賽門鐵克未來充滿信心。(美籍華人王嘉康創辦的企業軟體公司，聯合國國際電 (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 8 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，就如地緣政治考量，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 年起就全心全力專注在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，以及基於比原廠更熟悉用戶使用情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機構的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮詢的資安策略夥伴以及總是第一個被想到的求助諮詢對象。
保安資訊連絡電話：0800-381-500。

業界公認 保安資訊--賽門鐵克解決方案專家

🇨🇵 We Keep IT Safe, Secure & Save you Time, Cost 🇨🇵

服務電話：0800-381500 | +886 4 23815000 | http://www.savetime.com.tw