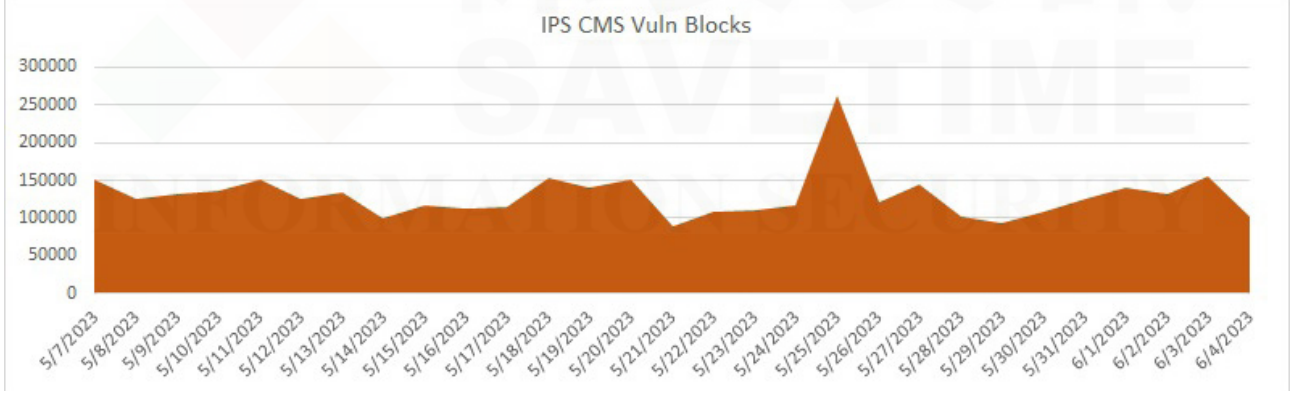
IPS～補強內容管理系統(CMS，Content Management System)漏洞的安全網

2023 年 6 月 5 日發布

WordPress、Joomla、Drupal……等內容管理系統 (CMS，Content Management System) 被廣泛用於建立和管理網站。它們的受歡迎程度意味著大量網站建立在這些平台上，使它們成為攻擊者覬覦的目標。這些平台是複雜的軟體系統，具有各種元件、佈景主題 (Themes)、外掛 (Plugins) 和多元的模組，通常由不同的開發人員所建立。這種複雜性可能會引入可被威脅者濫用的漏洞。隨著大量可用的第三方主題和外掛的出現，確保每個元件的安全變得非常具有挑戰性。

不幸的是，許多網站所有者並沒有保持他們的 CMS 及其組件是最新，這可能會使漏洞得不到修補，從而使攻擊者更容易利用已知的安全漏洞。通常 CMS 漏洞都有詳細記錄，攻擊者會主動搜索運行老舊版本的網站。大多數攻擊者會利用自動化工具來開採利用這些漏洞，從而更容易發動廣泛的攻擊。他們可以在網際網路上掃描運行特定 CMS 版本的網站、識別漏洞並大規模發起自動化攻擊。

賽門鐵克入侵防禦系統(IPS) 無時不刻一直在主動攔阻試圖利用這些 CMS 漏洞利用的威脅。



駭客最喜歡攻擊伺服器，特別是面向網際網路的公眾服務主機的先天脆弱性。在我們『上個月 IPS 做了什麼來保護伺服器？』5 月份的公告中，我們 IPS 網路層防護成功攔阻在 12.2K 伺服器上共 140 萬次的 CMS 漏洞利用嘗試。攻擊者從未鬆懈，一直樂此不疲。

多年來，CMS 漏洞與各種威脅和惡意活動有關。已經出現的一些常見威脅包括：

- 未經授權的存取：利用 CMS 漏洞可以為攻擊者提供對網站後端的未經授權存取，從而使他們能夠控制內容管理系統。此存取可用於操縱網站內容、竊取資料或執行其他惡意活動。
- 篡改：可利用 CMS 漏洞透過注入未經授權內容或修改現有內容來篡改網站。攻擊者可能會用惡意或仇視內容置換網站的原始內容，從而對網站所有者或組織的聲譽造成損害。
- 資料外洩：CMS 漏洞可能導致資料外洩，攻擊者可以存取存儲在網站上的敏感資訊。這可能包括用戶憑證、個人資料、財務數據或專有業務訊息。被盜資訊可用於身份盜用、金融欺詐或在黑市上出售。
- 散播惡意軟體：利用 CMS 漏洞可以讓攻擊者將惡意程式碼注入網站。此程式碼可用於將惡意軟體散播給毫無戒心的造訪者，駭入他們的電腦並可能將感染鏈傳播到其他系統。
- 網路釣魚攻擊：可以開採利用 CMS 漏洞來發動網路釣魚行動。攻擊者可以建立看似合法但目的是竊取用戶憑證／帳密或機敏資訊的虛假登錄頁面或表單。網路釣魚攻擊可能導致身份盜用、財務損失或未經授權存取其他帳戶。
- SEO (搜尋引擎最佳化) 垃圾郵件：可以利用 CMS 漏洞將隱藏鏈接或關鍵字注入網站內容。這通常是為了 SEO (搜索引擎最佳化) 垃圾郵件目的，攻擊者操縱搜索引擎排名來推廣他們自己的網站或產品。
- 分散式阻斷服務 (DDoS)：可利用 CMS 漏洞對網站發起 DDoS 攻擊。透過利用 CMS 或相關外掛程式中的弱點，攻擊者可以用大量請求使網站伺服器過載，從而使合法用戶無法造訪該網站。

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 **零時差**防護技術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：

- Web Attack: WordPress Plugin XSS Attempt
- Web Attack: WordPress XMLRPC Malicious Pingback Request
- Web Attack: Wordpress Arbitrary File Download 4
- Web Attack: Sourcecodester System CVE-2020-29227
- Web Attack: Joomla Component Local File Inclusion
- Attack: Web CMS Multiple Sql Injection
- Web Attack: Drupal Core RCE CVE-2018-7602
- Web Attack: WordPress Plugin Path Traversal Attempt
- Web Attack: Wordpress Arbitrary File Download CVE-2003-1599
- Attack: Wordpress Duplicator Plugin Unauthenticated Arbitrary File Download

欲瞭解更多有關於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**。