固若金湯的IPS防護技術，提供目錄遍歷攻擊堅若磐石的保護

2024 年 6 月 18 日發布

目錄遍歷(Path Traversal)／路徑跨越(path traversal)漏洞

目錄遍歷漏洞又稱路徑跨越漏洞，是網路應用程式中的一個安全性漏洞，允許攻擊者存取網頁伺服器根目錄之外受限制存取的檔案和目錄。

目錄遍歷攻擊操弄網頁應用程式中引用檔案路徑的變數。攻擊者修改路徑變數，以便在目錄結構中向上移動或瀏覽到不同的目錄。通常會使用特定的序列來完成，例如：在 Unix 和 Windows 系統中分別使用『.../』或『...\』。攻擊者可能會在網址或輸入欄位中使用這些序列，試圖誘騙伺服器從文件的根目錄之外傳回檔案。

目錄遍歷漏洞是對使用者輸入的過濾／驗證不足造成的。目錄遍歷漏洞可能存在於網頁伺服器軟體和檔案中，也可能存在於伺服器上執行的應用程式碼中。

目錄遍歷在 CWE 前 25 個最危險軟體弱點清單和前 25 個頑固弱點列表中排名第 8。美國網路安全暨基礎設施安全局 CISA 在「已知成功利用漏洞列表(the Known Exploited Vulnerabilities Catalog-KEV)」目錄中列出 50 多個目錄遍歷漏洞。因此，目錄遍歷漏洞仍然是軟體產品中長期存在的一項缺陷。

目錄遍歷攻擊的危害程度

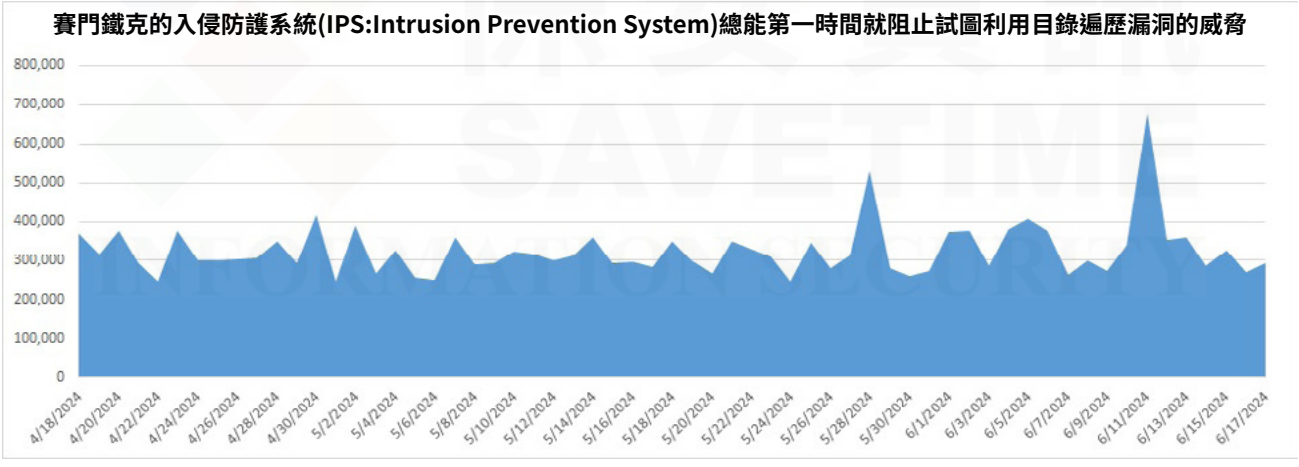
目錄遍歷攻擊對網頁伺服器和應用程式的安全性和完整性構成重大威脅：

- 目錄遍歷可導致未經授權存取儲存在網頁根目錄以外檔案中的敏感資訊。這可能包括系統檔案、設定檔甚至使用者資料。未經授權存取機密資料是對隱私的直接侵犯，並可能導致資訊失竊。
- 攻擊者可以讀取、修改或刪除關鍵檔，造成嚴重的系統故障或服務中斷。可能導致嚴重的停機、生產力損失甚至經濟損失。
- 成功的目錄遍歷攻擊可為攻擊者提供實施破壞性攻擊的能力。例如：存取某些系統檔可以提供有關伺服器結構、配置和安全措施的寶貴資訊。綜合來看，這些資訊可用在未來建立更複雜的攻擊。

目錄遍歷是一種嚴重的安全風險，會導致網頁伺服器和應用程式的隱私性、完整性和可用性嚴重受損。

賽門鐵克的網路層的防護技術

賽門鐵克的入侵防護系統 (IPS：Intrusion Prevention System) 總能第一時間阻止試圖利用目錄遍歷漏洞的威脅。IPS 平均每天可攔截超過 1 萬 3,000 台電腦，共高達 34 萬次的目錄遍歷攻擊。



賽門鐵克與時俱進的創新多層次零時差防護技術經證實可以有效防禦這些攻擊，包括但不限於以下措施：

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: Generic Directory Traversal 5
- Attack: Generic Directory Traversal 2
- Web Attack: Directory Traversal Exploitation Attempt
- Web Attack: Adobe Coldfusion Directory Traversal Vulnerability
- Attack: HTTP Apache Tomcat UTF-8 Dir Traversal CVE-2008-2938
- Web Attack: Adobe ColdFusion Directory Traversal Vulnerability CVE-2013-0629
- Web Attack: Apache Tomcat Directory Traversal CVE-2000-1210
- Web Attack: SCO Skunkware ViewSrc Directory Traversal CVE-1999-0174
- Web Attack: Fortinet FortiOS Directory Traversal CVE-2018-13379
- Web Attack: IBM Tivoli Directory Server Directory Traversal Vulnerability CVE-2004-2526

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**。