ToolShell：嚴重的 SharePoint 零日漏洞已遭到廣泛攻擊

2025 年 7 月 21 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

Symantec 產品已封鎖 CVE-2025-53770 零日漏洞的利用嘗試

微軟已針對 SharePoint 的零時差漏洞進行部分修補。此漏洞 (CVE-2025-53770) 稱為 ToolShell，會影響內部已部署的 SharePoint 伺服器，讓攻擊者在未經認證情況下存取受影響的伺服器，從而遠端執行程式碼並存取所有內容和檔案系統。雖然 2019 版 SharePoint Server 和 SharePoint Server Subscription Edition 已經釋出修補程式，但 SharePoint Server 2016 版仍未修補。

微軟在其有關漏洞的指引中表示，「已知有針對企業內部 SharePoint Server 客戶的主動攻擊」。微軟並未提供進一步資訊，說明這些攻擊背後的主腦是誰。

新的零時差漏洞是最近修補過的漏洞 CVE-2025-49704 之變種，CVE-2025-49704 已於 2025 年 7 月修補過。

防護

賽門鐵克產品已透過下列網路防護功能阻擋利用此漏洞：

網路攻擊： Microsoft SharePoint CVE-2025-49704。

相關漏洞

第二個相關漏洞 (CVE-2025-53771) 也已修補。這是一個路徑遍歷的 bug，允許授權的攻擊者透過網路執行欺騙。它也是最近修補過漏洞 (CVE-2025-49706) 的變種，修補程式包含更強大的保護功能，以防止利用較舊的漏洞。

緩解措施與指引

除了立即更新至最新版本的 SharePoint 外，美國網路安全與基礎建設安全局 (CISA) 建議使用者監控以下路徑的 POSTs 指令參數：

/_layouts/15/ToolPane.aspx?DisplayMode=Edit

也建議使用者針對下列 IP 位址進行掃描：107.191.58[.]76、104.238.159[.]149 和 96.9.125[.]147，尤其是在 2025 年 7 月 18-19 日之間。

防護方案／緩解措施

網路防護

網路攻擊： Microsoft SharePoint CVE-2025-49704。

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (Indicators of Compromise)

如果 IOC 是惡意的並且我們能夠使用該檔案，Symantec Endpoint 產品將檢測並阻止該檔案。

注意：如下 IP 位址是已知掃描 CVE-2025-53770 和利用 CVE-2025-53770活動 IP 的集合。

107.191.58[.]76
104.238.159[.]149
96.9.125[.]147
103.186.30[.]186
108.162.221[.]103
128.49.100[.]57
154.47.29[.]4
162.158.14[.]149
162.158.14[.]86
162.158.19[.]169
162.158.90[.]110
162.158.94[.]121
162.158.94[.]72
18.143.202[.]126
18.143.202[.]156
18.143.202[.]185
18.143.202[.]204
45.40.52[.]75

關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

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，以及基於比原廠更孰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組織的信賴，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、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：**0800-381-500**。