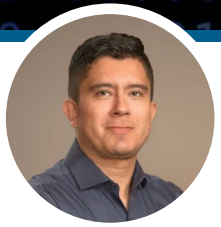
防止 Outlook 的權限擴張

2023 年 4 月 12 日發布｜專家觀點



Tom Blauvelt
網路安全架構師

使用 Symantec Endpoint Security Complete (SESC) 進行檢測和保護

全球約 10% 的軟體漏洞被歸類為嚴重漏洞，導致受影響的系統損失慘重。脆弱性的系統可能會嚴重影響完整性、機密性和可用性，損害業務運作並威脅使用者資料的安全。這就是 Microsoft 於 2023 年 3 月 14 日宣布漏洞 CVE-2023-23397 的情況，該漏洞也稱為「Microsoft Outlook 特權提升漏洞」。根據通用漏洞評分系統 (CVSS)，CVE-2023-23397 被評為嚴重，得分為 9.8(滿分為 10)。此基本評分指標意味著該漏洞可遠端利用、複雜性較低且無需用戶互動。換句話說，越容易被利用，對資安鐵三角 CIA(機密性、完整性、可用性) 的影響就越大。

採用 Symantec Endpoint Security Complete(SESC) 的客戶可以使用 SESC 單一代理程式來減少攻擊面、預防攻擊、預防安全漏洞、端點偵測和回應 (EDR) 以及漏洞防護。

透過端點安全和偵測，Broadcom 透過提供 CVE-2023-23397 影響的緩解和可見性來保護我們的客戶。

Symantec Endpoint Security Complete：偵測功能

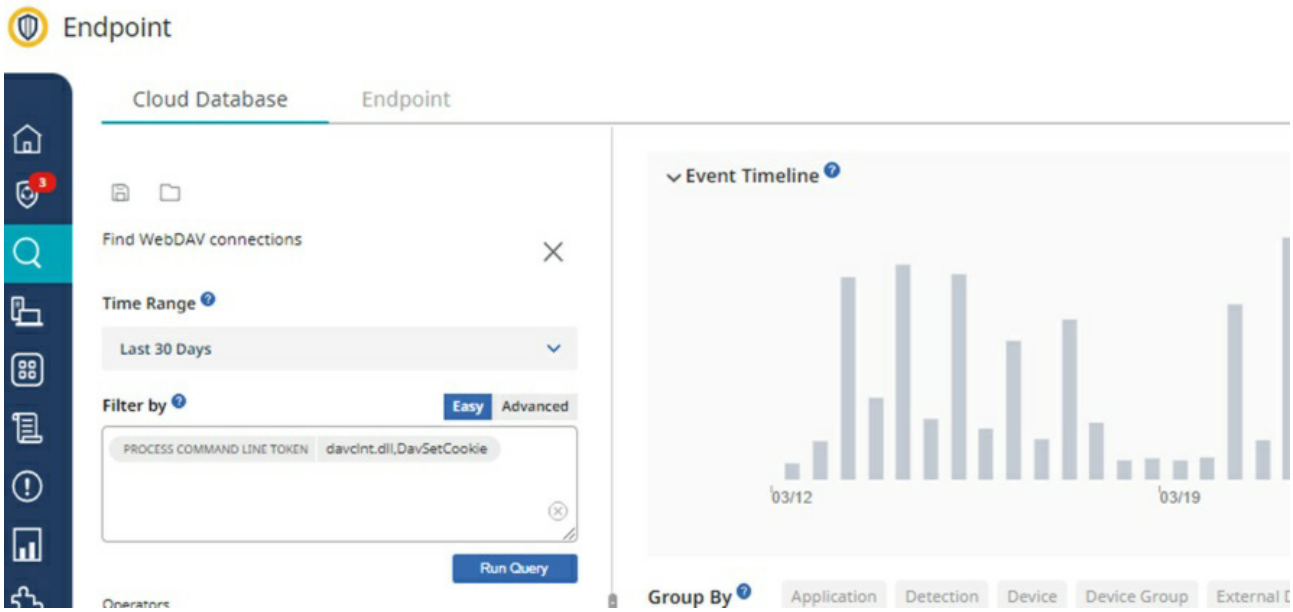
透過分析 CVE-2023-23397，Infolock 能夠評估使用 SESC 客戶目前的檢測和緩解資源。這包括端點偵測和回應、合規性、入侵防禦和防火牆等政策。

端點和回應政策：偵測 WebDAV 連接

如果您的組織封鎖 SMB 到 Internet 的流量，在此漏洞被利用的情況下，Windows 會嘗試透過 WebDAV 的方式來完成外部連接。

- SESC 分析報告可以匯出 CSV 文件，透過查詢：**process.cmd_line.token:davclnt.dll**，**DavSetCookie** 來分析可疑流量的潛在外部目的地

在 **Investigative** 標籤上，選擇 **TIME**、**DESCRIPTION**、**DEVICE NAME**、**PROCESS COMMAND LINE** 和 **USER** 欄。



圖：查詢路徑範例

底下資訊會在分析報告的 Process Command Line 欄中顯示，可以做為 CVE-2023-23397 漏洞被利用的證據。

rundll32.exe C:\Windows\system32\davclnt.dll,DavSetCookie <外部連接目標的IP-FQDN > hxxp://<外部連接目標的IP-FQDN >/shared-folder/sound.wav

主機完整性政策（也稱為合規性政策）

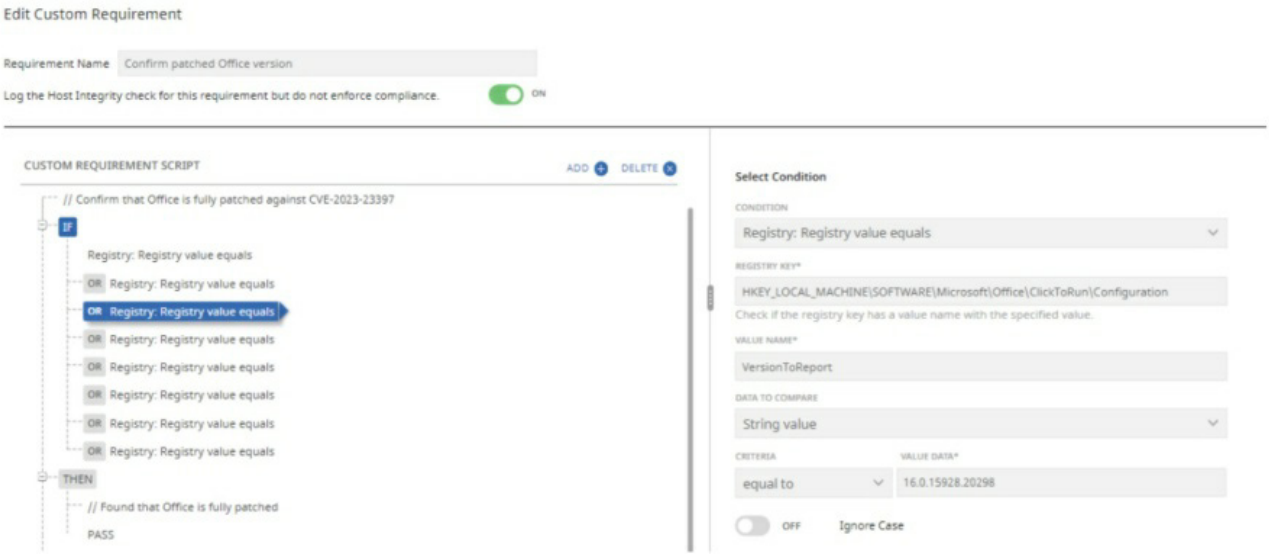
主機完整性政策包括自定義的需求，用於檢查設備的合規性。例如：您可以定義一個需求來檢查 Windows 登錄表鍵或登錄表值的存在。

為了檢查此特定漏洞，我們制定了兩項政策：驗證公司內可用的 Office 版本是否容易受到漏洞影響，以及驗證如何識別入侵指標 (IoC) 。

- ***驗證是否部署了修補後的 Outlook 版本***。

通過使用 Click-to-Run 登錄表鍵，主機完整性政策可以用來確定特定的登錄表值是否屬於已修補的 Office 版本。

在這種情況下，要使用的條件是『Registry: Registry value exists』。該值是基於登錄表中可用的 Click-to-Run 版本。



圖：驗證是否部署了修補後的 Outlook 版本

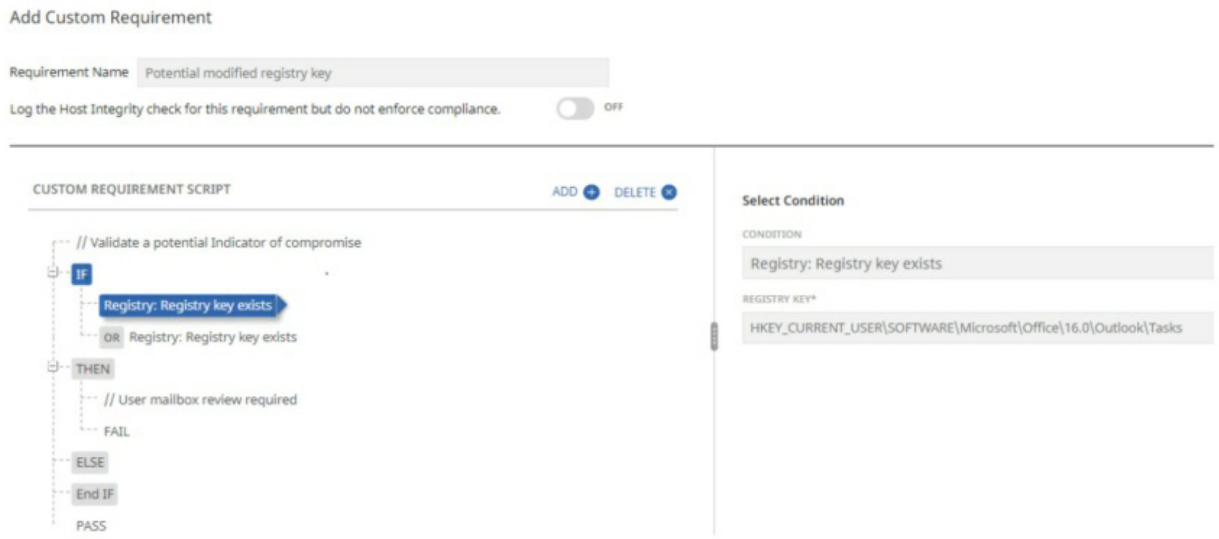
・入侵指標

透過分析特定登錄表鍵的存在，可以作為使用者收到工作或提醒的證據，在正常情況下該登錄表鍵不應存在。

透過設定 SESC 的主機完整性原則和條件『Registry: Registry value exists』，可以確定潛在的入侵指標 (IoC) 存在，例如：

HKCU\Software\Microsoft\Office\<OUTLOOK 版本>\Outlook\Tasks

HKCU\Software\Microsoft\Office\<OUTLOOK 版本>\Outlook\Notes



圖：尋找入侵指標 (IoC)

入侵防禦政策(Intrusion Prevention Policies，IPS)

賽門鐵克安全回應中心目前包含兩項稽核檢測的 IPS 簽章。分別是 Audit：SMBv1 NTLM Authentication Attempt 和 Audit：SMBv2 NTLM Authentication Attempt 。

這兩個簽章都能檢測私有 IP 到公共 IP 的 NTLM 認證嘗試。這是因為 Windows 作業系統在與外部主機連接時會自動發送 NTLM 雜湊。攻擊者可以利用此雜湊進行破解或重播攻擊。

考慮到稽核簽章只會記錄事件，因此可以根據需要變更檢測後的操作。

防火牆政策

一般經驗法則是阻止來自TCP 445/SMB 的對外網路連線，以防止 NTLM 驗證訊息傳送到遠端檔案分享。

SESC 的防火牆政策需要建立兩個主要的安全性和網路因素。

1. 決定哪些 Internet 資源將被允許進行對外的 SMB 連線。

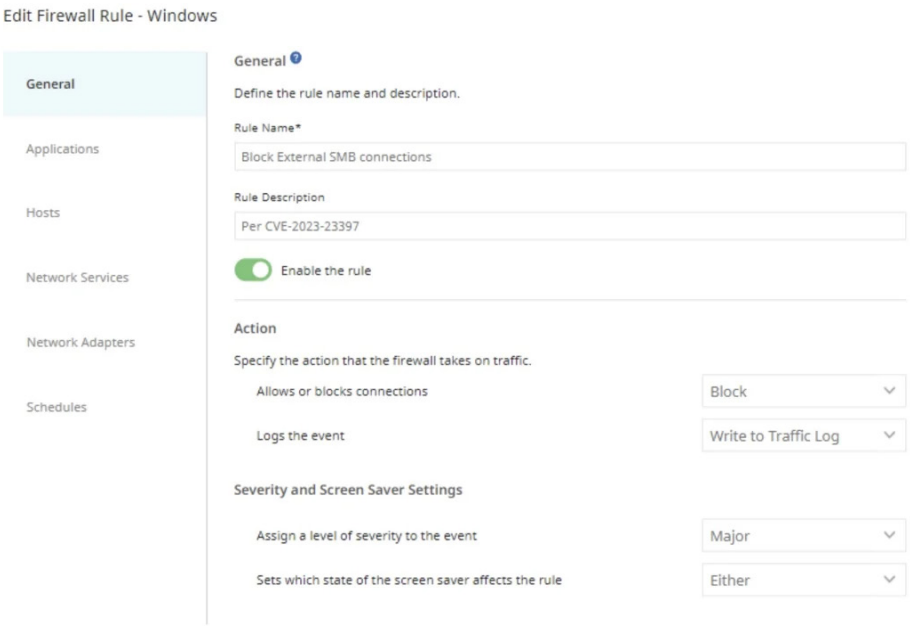
   從「Policy Components」區域建立所需的 SESC 主機群組，並列出內部／授權的 SMB 連線資源。

2. 使用日誌來記錄對外的 SMB 連線應該阻止或允許。

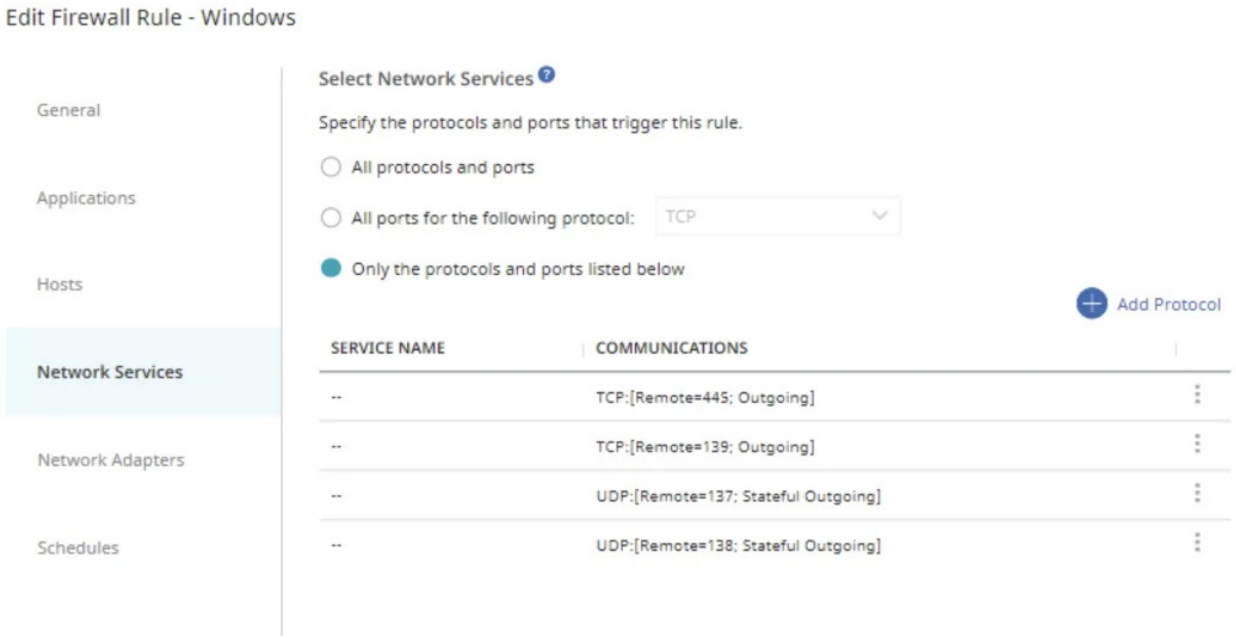
   如果您的遠端工作人員需要對未連接 VPN 的資源進行 SMB 存取，則日誌記錄政策可以幫助您識別非 VPN 裝置上發生的風險。

一旦確定了上述因素，防火牆政策應包含以下兩條規則：

- ***允許內部（或其他經授權的）SMB流量的規則***
- ***限制對外SMB流量流向未經授權的目的地的阻止規則***



範例 2. 建立防火牆政策



範例 1. 建立防火牆政策

擁有近二十年資訊安全領域的經驗，我一直親身參與協助全球的組織對抗網路攻擊。透過使用賽門鐵克企業安全解決方案，我能夠為客戶提供對安全威脅的可見性、保護和控制，並且能夠減輕，甚至完全防止網路攻擊的影響，無論嚴重程度如何。

關於作者

Tom Blauvelt
網路安全架構師

Tom Blauvelt 是賽門鐵克策略團隊的網路安全架構師。他在技術和策略方面數十年的工作經驗使他能夠與 CISO 和 SOC 分析師合作，針對當今不斷變化的威脅情勢客製化解決方案。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/protecting-against-outlook-elevation-privilege-escalation

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**。