

安全訪問終端安全評估配置檔案作業系統版本檢查行為

目錄

問題

使用終端安全評估配置檔案配置遠端訪問VPN(RAVPN)的Cisco安全訪問時，管理員可能會遇到作業系統安全評估設定未在可用覈取方塊中顯示較新Windows 11版本的情況。具體來說，OS版本檢查只能顯示Windows 11 24H2之前的選項，而更新版本（如Windows 11 25H2）未明確列為狀態配置檔案配置介面中的單個覈取方塊。

這會產生不確定性，說明運行未經檢查的OS版本的終端在VPN連線嘗試期間的行為，尤其是當觀察到Windows 11 25H2終端成功建立VPN連線（儘管在終端安全評估配置檔案配置中沒有明確的覈取方塊選擇）時。

有問題的配置區域位於：安全(Secure)>終端安全評估配置檔案(Endpoint Posture Profiles)> VPN連線(VPN Connection)>作業系統(Operating System)。

環境

- 為遠端接入VPN(RAVPN)配置的Cisco安全接入平台
- 配置了作業系統版本檢查的終端安全評估配置檔案
- 運行包括25H2在內的各種版本的Windows 11終端
- 狀態配置檔案作業系統設定，顯示在Windows 11 24H2結束的可用覈取方塊

解析

Windows 11 25H2終端在未選中明確覈取方塊的情況下成功連線時觀察到的行為是由終端狀態配置檔案作業系統設定中的最新選擇機制引起的。

瞭解作業系統版本匹配行為

當終端作業系統版本未明確與終端安全評估配置檔案中的任何單個版本覈取方塊匹配時，預期的預設行為通常會在VPN連線嘗試期間導致身份驗證錯誤。但是，狀態配置檔案系統包含Latest選項，該選項包含除了明確列為單個覈取方塊之外的較新OS版本。

驗證包含的作業系統版本

要確認Latest選項中包含哪些作業系統版本，請執行以下操作：

步驟 1:導航到終端安全評估配置檔案配置。Access Secure > Endpoint Posture Profiles > VPN Connection > Operating System。

步驟 2:檢查Latest選項資訊。查詢Latest選項旁邊的資訊工具提示(i)圖示，以檢視此類別中包含哪些特定的OS版本。

未選中作業系統版本的預期行為

對於單個覈取方塊或Latest選項未覆蓋的作業系統版本，系統會實施狀態要求並阻止VPN連線。在這種情況下，終端在VPN連線過程中會遇到身份驗證錯誤，因為不符合狀態檢查要求。

原因

可用的單個作業系統版本覈取方塊與來自較新作業系統版本的成功連線之間存在明顯差異，因為Cisco Secure Access使用Latest選擇機制，該機制自動包括較新的作業系統版本。Windows 11 25H2包含在Latest類別下，允許這些終端滿足終端安全評估要求，即使在配置介面中未明確列為單個覈取方塊選項時也是如此。此設計允許終端安全評估系統適應新的作業系統版本，而無需立即更新使用者介面中的各個覈取方塊清單。

相關內容

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。