01_外部專案 - 專案資訊 #1068

專案資訊 # 1064 (New-新增): 2025-PenTest

Dangerous Permisson over GPO that applies to object with high privileges

2025-11-10 13:28 - Joy Liao

狀態:	Resolved-解決	**開始日期:**	2025-08-01
優先權:	Normal	**完成日期:**	2025-12-31
被分派者:	益利 周	**完成百分比:**	100%
分類:		**預估工時:**	0:00 小時
版本:		**耗用工時:**	0:00 小時

概述

NN　bookmark202505281055547217281479l7　"Dangerous Permisson over GPO that applies to object with high privileges

All domain users can modify GPO that will affect an OU containing domain admins."　Domain dominance is possible if adversary inserts malicious scripts into the affected GPO, which will be automatically executed when users in the affected Ous logon.　"It is imperative that the permissions assigned to GPOs that will be applied to objects with high privileges be reviewed with the utmost care. These permissions must be granted only for the minimum necessity.

"

歷史

#1 - 2025-11-10 13:34 - Joy Liao

- 完成日期 設定為 2025-12-31

- 被分派者 設定為 益利 周

- 開始日期 從 2025-11-10 變更為 2025-08-01

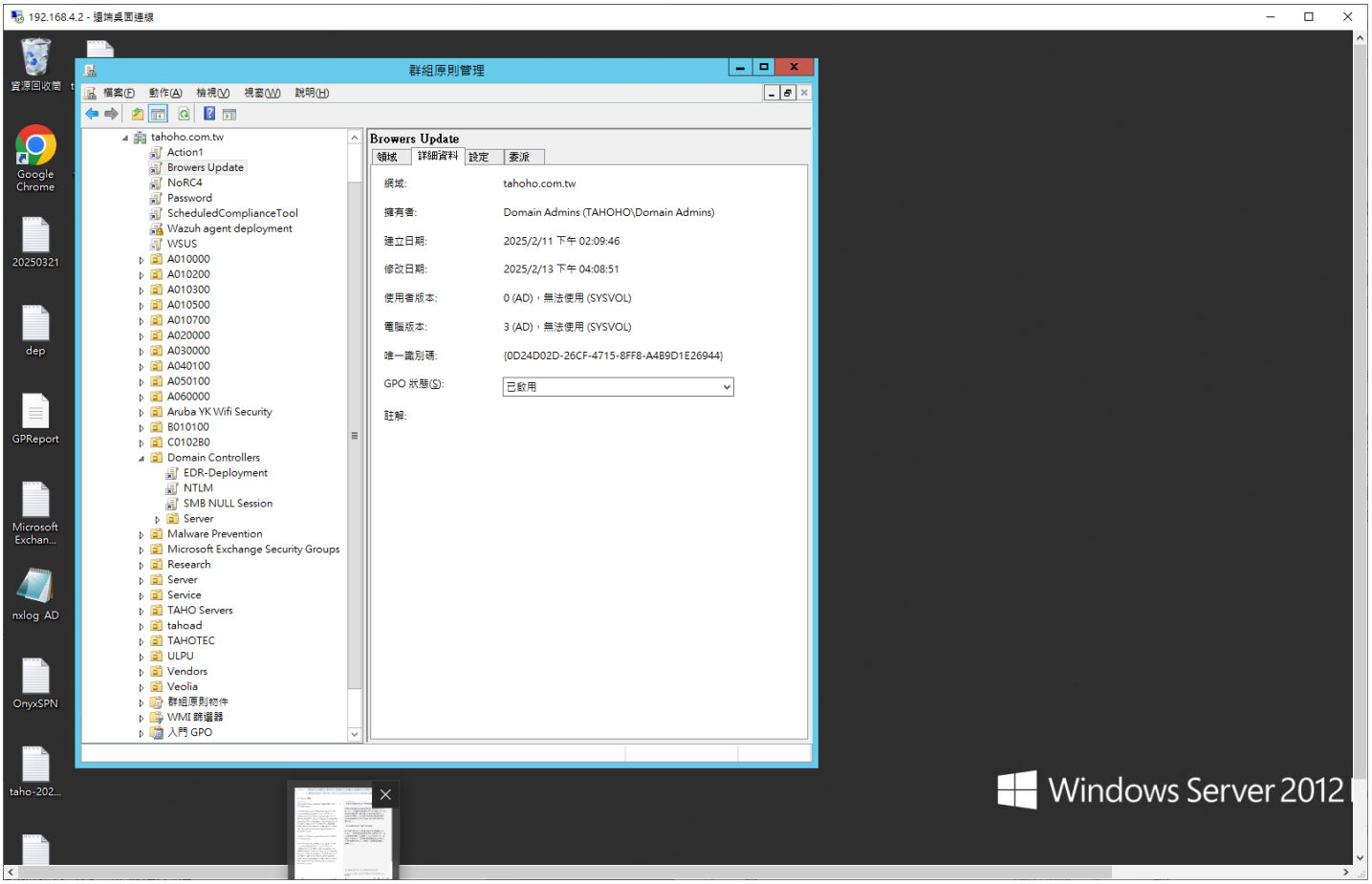
#2 - 2025-11-28 11:04 - 益利 周

- 檔案 clipboard-202511281105-zyyow.png 已新增

- 狀態 從 New-新增 變更為 Resolved-解決

- 完成百分比 從 0 變更為 100

1. 識別受影響的 GPO 和目標 OU
首先，您需要確定哪些 GPO 連結到了包含高權限帳戶或群組的 OU。
可行之做法：
使用 Group Policy Management Console (GPMC) 進行分析：
開啟 GPMC (gpmc.msc)。
導航至包含高權限帳戶的目標 OU（例如 Domain Admins 所在的 Administrators 容器或特定的管理 OU）。
查看「已連結的群組原則物件」標籤頁，記下列出的 GPO 名稱。
稽核 GPO 的委派設定：
針對每個已識別的 GPO，導航到「委派」標籤頁。
檢查哪些使用者或群組擁有「編輯設定、刪除、修改安全性」或「編輯設定」的權限。尋找任何非管理員使用者或群組。
2. 移除不必要帳戶的修改權限
一旦識別出錯誤配置的 GPO，必須立即移除標準使用者的寫入權限。
可行之做法：
實施嚴格的最小權限原則：
在 GPMC 中，右鍵點擊受影響的 GPO，選擇**「內容」** -> *「安全性」*標籤頁 -> 「進階」。
針對「Domain Users」、「Authenticated Users」或任何標準使用者群組，移除所有「寫入」、「修改權限」或「完全控制」的「允許」權限。
重要： 確保這些群組僅擁有「讀取」權限，這允許原則應用到他們的帳戶，但不允許他們修改原則本身。
確保只有 Domain Admins、Enterprise Admins 和內建的 Administrators 群組擁有完全控制或寫入權限。
限制 GPO 連結的修改權限：
除了限制 GPO 本身的權限，還需要限制 OU 層級的權限。確保只有管理員可以連結或取消連結 GPO 到高權限 OU。
3. 實施長期監控與流程控制
防止未來再次發生配置錯誤，並監控潛在的惡意活動。
可行之做法：
監控 GPO 的變更：
設定詳細的稽核，監控對這些敏感 GPO 的任何修改。在 Windows 安全事件日誌中，監控 Event ID 4662（對物件執行的作業）或使用 GPO 特定稽核事件來追蹤變更。
使用 GPO 版本控制和備份：
定期備份這些關鍵 GPO。在 GPMC 中使用「管理備份」功能，並在發現未經授權的變更時能夠快速還原到安全的版本。
標準化變更管理流程：
建立嚴格的 IT 政策，規範所有影響高權限 OU 的 GPO 變更都必須經過嚴格的測試、審批和記錄，並由授權的管理員執行。



檔案

clipboard-202511281105-zyyow.png	193 KB	2025-11-28	益利 周