01_外部專案 - 專案資訊 #1088

專案資訊 # 1064 (New-新增): 2025-PenTest

Dangerous Permission over adminSDHolder

2025-11-10 13:33 - 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

bookmark202505271715271727489203 5 "Dangerous Permission over adminSDHolder

" "Granting dangerous permissions over the adminSDHolder container enables attackers to bypass security protections for privileged accounts. Since adminSDHolder automatically resets permissions on protected groups, attackers with write access can establish persistent backdoors in critical admin groups, maintaining undetected control even after password rotations.

" "It is essential to meticulously review the permissions assigned to the adminSDHolder object for non-administrative domain objects, ensuring that permissions are granted only for the minimum necessary.

"

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

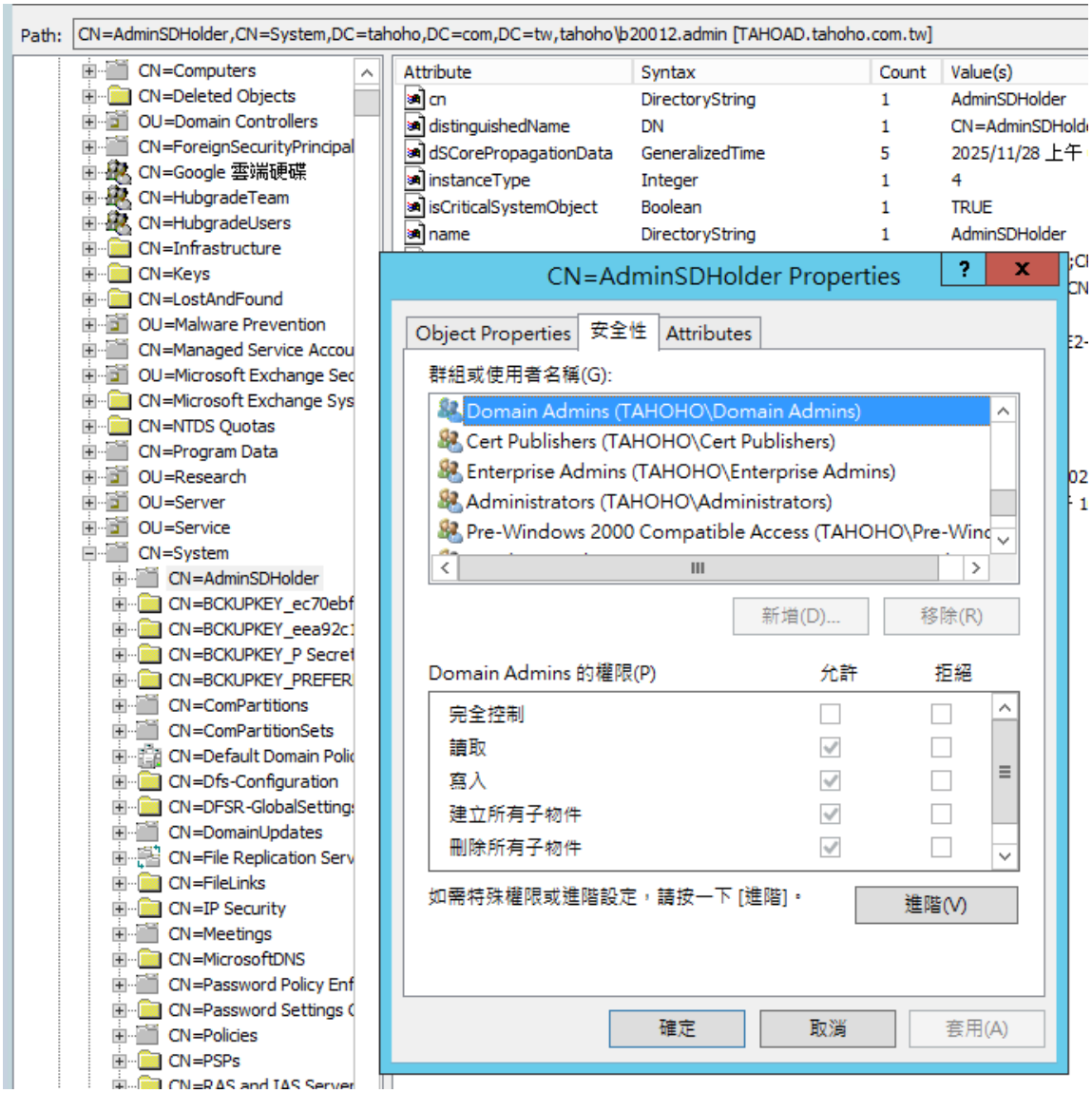
#2 - 2025-11-28 10:00 - 益利 周

- 檔案 clipboard-202511281000-fvkh0.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

adminSDHolder 物件是 Active Directory 中保護高權限帳戶的關鍵安全機制。它就像一個「權限範本」，每小時會將其自身的 ACL (存取控制列表) 強制複製到所有受保護的管理員群組（如 Domain Admins, Enterprise Admins, Administrators 等）。
如果非管理員帳戶對 adminSDHolder 擁有寫入（Write）權限，攻擊者就可以修改這個範本，從而在所有受保護的管理群組中建立永久性的後門，即使密碼重設也無法清除。這是一個極其危險的配置錯誤。
核心改善目標是：確保只有最高層級的、受信任的管理員群組對 adminSDHolder 具有寫入權限，並嚴格限制其他所有帳戶的存取。
以下是針對此問題的具體改善因應做法：
1. 識別與稽核目前的 adminSDHolder 權限
2. 移除非必要帳戶的危險權限
開啟 ADSI Edit (adsiedit.msc)。
連線到預設命名內容。
導航至 CN=AdminSDHolder,CN=System,DC=yourdomain,DC=com。
右鍵點擊該物件，選擇**「內容」，然後切換到「安全性」**標籤頁。
仔細審查列表中的群組。針對「Authenticated Users」、「Domain Users」或任何其他非特權管理員群組：
移除任何允許「完全控制」(Full Control)、「寫入所有屬性」(Write All Properties) 或「修改權限」(Modify Permissions) 的「允許」(Allow) 選項。
確保僅剩以下群組擁有寫入或修改權限： Domain Admins, Enterprise Admins, Administrators (內建), SYSTEM。



檔案

clipboard-202511281000-fvkh0.png	96.3 KB	2025-11-28	益利 周