01_外部專案 - 專案資訊 #1085

專案資訊 # 1064 (New-新增): 2025-PenTest

Dangerous Permission over Privileged Objects Containers

2025-11-10 13:32 - Joy Liao

狀態:	In process-進行中	**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:**	30%
分類:		**預估工時:**	0:00 小時
版本:		**耗用工時:**	0:00 小時

概述

bookmark202505281134405905259118 82 "Dangerous Permission over Privileged Objects Containers

" Unrestricted access to privileged containers lets attackers hijack admin accounts and subvert security safeguards, leading to undetected domain dominance. "It is essential to meticulously review the permissions assigned to the privileged object containers 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 10:47 - 益利 周

- 狀態 從 New-新增 變更為 In process-進行中

- 完成百分比 從 0 變更為 30

核心改善目標是：嚴格限制對特權 Active Directory 容器的存取，實施最小權限原則，並將權限委派標準化。
以下是針對此問題的具體改善因應做法：
1. 識別與定義特權容器
首先，需要明確指出哪些 AD 物件被視為「特權容器」。通常包括以下幾個：
Administrators **容器（預設情況下存放** Domain Admins, Enterprise Admins **等群組）。**
Users **容器（存放許多內建的、高權限的服務帳戶或預設帳戶，如** krbtgt）。
任何包含委派了高權限管理帳戶的自定義 OU。
AdminSDHolder **物件本身。**
2. 稽核現有權限配置
在進行任何修改之前，必須先了解目前非管理員帳戶擁有哪些不必要的權限。
可行之做法：
使用工具分析 ACLs**： 使用內建工具** DSACLS **或** PowerShell **腳本來匯出特權容器的存取控制列表**
(ACLs)。**仔細審查哪些非管理員使用者或群組被授予了「寫入屬性」、「建立子物件」、「刪除子物件」或「修改成員資格」等權限。**
專注於「繼承」的權限： 檢查是否存在從父層級繼承下來的過度許可權限，這些權限可能會影響特權帳戶。
3. 實施嚴格的權限移除與委派重構
這是最關鍵的修正步驟。目標是移除所有非管理員對特權容器的寫入或修改權限。
可行之做法：
移除所有不必要的「允許」權限：
針對特權容器，明確地從「Authenticated Users**」、「**Domain Users**」或任何其他標準使用者群組的** ACL **中移除寫入** (Write) **或修改成員資格** (Modify Membership) **的權限。**
使用 ADSI Edit **或** ADUC **的「安全性」標籤頁，確保這些群組的權限僅限於「讀取」。**
使用 AD **保護機制** (AdminSDHolder) **的強制性：**
理解並利用 AdminSDHolder **機制。該物件定義了一個模板** ACL，**每隔一小時會自動覆蓋（強制繼承）所有受保護群組的權限設定。確保** AdminSDHolder **上的** ACL **配置正確且受限，這是自動化保護特權帳戶的關鍵。**
遵循最小權限原則 (PoLP)**：**
重新設計委派模型。不要在容器層級給予寬泛的權限。精確地授予執行特定任務所需的最低權限。