01_外部專案 - 專案資訊 #1089

專案資訊 # 1064 (New-新增): 2025-PenTest

Dangerous Permission over DNSAdmins Group

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

bookmark202505271645298197567439 71 "Dangerous Permission over DNSAdmins Group

" Granting excessive permissions to the DNSAdmins group allows attackers to load malicious DLLs on domain controllers via DNS server modifications. This enables privilege escalation to Domain Admin, as compromised members can execute code on DCs, facilitating persistent backdoor access and control over DNS resolution. "It is imperative that the permissions assigned to the DNSAdmins group for non-administrative domain objects 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 09:36 - 益利 周

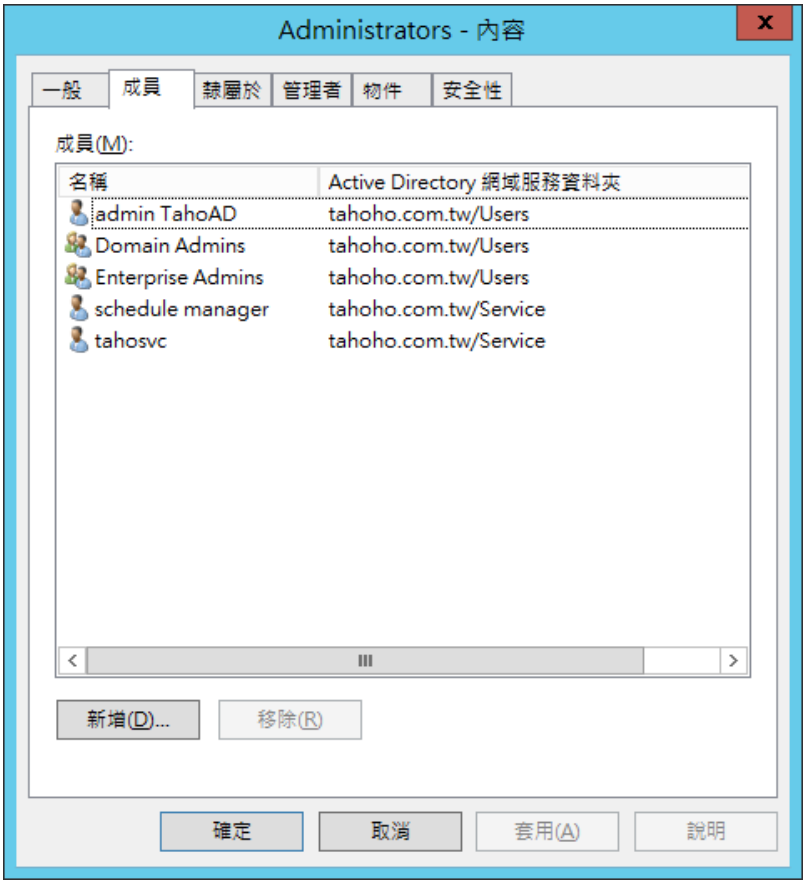
- 檔案 clipboard-202511280936-crt3g.png 已新增

- 狀態 從 New-新增 變更為 Resolved-解決

- 完成百分比 從 0 變更為 100

核心改善目標是：限制 DNSAdmins 群組的成員資格，並移除該群組在網域控制站上的本地管理權限，確保其權限僅限於管理 DNS 服務本身。
以下是具體的改善因應做法：
1. 限制 DNSAdmins 群組成員資格
最直接的緩解措施是確保只有絕對必要且受信任的管理員才屬於此群組。
可行之做法：
實施最小權限原則 (PoLP)： 徹底審查 DNSAdmins 群組目前的成員列表。移除所有非必要人員或服務帳戶。
專用帳戶管理： 成員應使用專門的管理員帳戶來執行 DNS 管理任務，而不是他們的日常使用者帳戶。
定期審核： 建立一個流程，定期（例如每季）審核該群組的成員資格，確保其組成仍然正確且必要。

2. 移除 DNSAdmins 在網域控制站上的特權
這是防止權限提升攻擊的關鍵步驟。雖然 DNSAdmins 需要權限來管理 DNS 服務，但他們不需要在網域控制站上擁有本地管理員權限。
可行之做法：
在每個網域控制站上，手動或透過腳本，從本地的 Administrators 群組中移除 DNSAdmins 群組。



檔案

clipboard-202511280936-crt3g.png	24.4 KB	2025-11-28	**益利 周**