

01_外部專案 - 專案資訊 #1073

專案資訊 # 1064 (New-新增): 2025-PenTest

SMB NULL Session Authentication allowed on Domain Controllers

2025-11-10 13:30 - 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			
"4.7.3			
CWE-16			
CWE-284			
" "SMB NULL Session Authentication allowed on Domain Controllers			
The SMB service on domain controllers allows users to authenticate using a NULL session, meaning that no user credentials need to be supplied to the server.			
" "An attacker may be able to read, delete or modify important data, and depending on the configuration, it could be possible to list information about the domain such as users and groups.			
" "Disallow the possibility to authenticate to the SMB server using NULL sessions, if this is not possible, do not store sensitive data in public shares.			
" "Status: Open			
CVSS-Score: 6.5			
CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N			
Fix Difficulty: Quick Win			
"			

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 - 2025-11-27 17:12 - 益利 周
- 檔案 clipboard-202511271712-72kpp.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.透過群組原則 (GPO) 停用 NULL 工作階段
- 2.套用至 網域控制站

- ▶ A020000
- ▶ A030000
- ▶ A040100
- ▶ A050100
- ▶ A060000
- ▶ Aruba YK Wifi Security
- ▶ B010100
- ▶ C0102B0
- ▶ Domain Controllers
 - EDR-Deployment
 - SMB NULL Session
 - Server
- ▶ Malware Prevention
- ▶ Microsoft Exchange Security Groups
- ▶ Research
- ▶ Server
- ▶ Service
- ▶ TAHO Servers
- ▶ tahoad
- ▶ TAHOTEC
- ▶ ULPU

SMB NULL Session

領域詳細資料設定委派

SMB NULL Session

資料收集: 2025/11/27 下午 05:08:55

電腦設定 (已啟用)

原則

Windows 設定

安全性設定

本機原則/安全性選項

網路存取

原則	設定
網路存取: 不允許 SAM 帳戶和共用的匿名列舉	已啟用
網路存取: 限制匿名存取具名管道和共用	已啟用

使用者設定 (已啟用)

沒有設定定義。

檔案

clipboard-202511271712-72kpp.png	49.3 KB	2025-11-27	益利 周
----------------------------------	---------	------------	------