

01_外部專案 - 專案資訊 #1074

專案資訊 # 1064 (New-新增): 2025-PenTest

Use of ""Pre-Windows 2000 Compatible Access

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
N bookmark2025052801463337292181788 "Use of ""Pre-Windows 2000 Compatible Access"" group
" "The “ Pre-Windows 2000 Compatible Access ” group allows its members read access to all user and computer objects in Active Directory, which can expose sensitive information. If an attacker gains membership in this group, they can exploit these permissions to gather valuable data and potentially elevate their privileges, compromising the security of the entire network.
" "Remove ""Anonymous Logon"" from the ""Pre-Windows 2000 Compatible Access"" group.
The Builtin\Pre-Windows 2000 Compatible Access group was originally designed to ensure backward compatibility for systems that predate Windows 2000 (Windows NT 4.0). It is imperative that this group exclusively encompass Authenticated Users (S-1-5-11). ADCS servers are automatically added to this group upon installation. Review any other membership to ensure that there is a business purpose of maintaining the membership. Should it not be necessary anymore, consider removing the membership."

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 17:21 - 益利 周
- 檔案 clipboard-202511271719-cigab.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
- 於 Pre-Windows 2000 Compatible Access 群組中
- 移除 "Anonymous Logon"

```
系統管理員: Windows PowerShell
Windows PowerShell 著作權 (C) 2014 Microsoft Corporation. 著作權所有，並保留一切權利。
PS C:\Windows\system32> Get-ADGroupMember -Identity "Pre-Windows 2000 Compatible Access"

distinguishedName : CN=TAHONAD,CN=Computers,DC=tahoho,DC=com,DC=tw
name               : TAHONAD
objectClass        : computer
objectGUID         : 9db08b0f-7b72-4f01-8500-8d91f522b8e5
SamAccountName     : TAHONAD$
SID               : S-1-5-21-845223939-707100287-312552118-20246

distinguishedName : CN=GSVR,OU=Server,OU=Domain Controllers,DC=tahoho,DC=com,DC=tw
name               : GSVR
objectClass        : computer
objectGUID         : ee5fab5-5b0d-4150-b828-c8daa26af235
SamAccountName     : GSVR$
SID               : S-1-5-21-845223939-707100287-312552118-15100

distinguishedName : CN=Exchange Domain Servers,CN=Users,DC=tahoho,DC=com,DC=tw
name               : Exchange Domain Servers
objectClass        : group
objectGUID         : 457f714f-6e3f-4273-becc-ce443c4733f6
SamAccountName     : Exchange Domain Servers
SID               : S-1-5-21-845223939-707100287-312552118-2887

distinguishedName : 
name               : Authenticated Users
objectClass        : 
objectGUID         : 00000000-0000-0000-0000-000000000000
SamAccountName     : Authenticated Users
SID               : S-1-5-11

distinguishedName : CN=TAHOAD,OU=Server,OU=Domain Controllers,DC=tahoho,DC=com,DC=tw
name               : TAHOAD
objectClass        : computer
objectGUID         : 26162ab1-dd41-41a6-8194-31a24410c353
SamAccountName     : TAHOAD$
SID               : S-1-5-21-845223939-707100287-312552118-4395

distinguishedName : CN=TAHONT,OU=Server,OU=Domain Controllers,DC=tahoho,DC=com,DC=tw
name               : TAHONT
objectClass        : computer
objectGUID         : 0ed87d60-cbf2-470c-9ac6-be0e81caab41
SamAccountName     : TAHONT$
SID               : S-1-5-21-845223939-707100287-312552118-1886

PS C:\Windows\system32>
```

名單中已無 Anonymous Logon

檔案

clipboard-202511271719-cigab.png	117 KB	2025-11-27	益利 周
----------------------------------	--------	------------	------