02_資安事件及異常紀錄 - 一般 #1134

INCGC-14067]-Medium-Possbile Kerberoasting Detected

2025-11-13 10:20 - 益利 周

狀態:	Closed-關閉	**開始日期:**	2025-11-13
優先權:	Normal	**完成日期:**	
被分派者:	益利 周	**完成百分比:**	100%
分類:		**預估工時:**	0:00 小時
概述			

歷史

#1 - 2025-12-01 11:51 - 益利 周

- 檔案 clipboard-202512011150-nwp9q.png 已新增

- 狀態 從 New-新增 變更為 Resolved-解決

- 被分派者 設定為 益利 周

- 完成百分比 從 0 變更為 100

Asset Owner : TWBU
Priority: Medium
Description:

Start Time: 2025-11-07 09:49:01 TST
End Time: 2025-11-07 09:49:01 TST
Rule Name: possbile_kerberoasting_detected
Rule Description: This rule detects TGS requests with RC4 for accounts with SPN set on the KDC. Due to the weak and unsalted nature of RC4, an attacker can brute force the acccount password offline and compromise it.
Priority: Medium
Log Type: WINEVTLOG
Event Type: USER_UNCATEGORIZED
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4769
Product Log ID: 1417188572
Opcode: 0
Channel: Security
Device: TAHOAD.tahoho.com.tw
Principal IP: 192.168.4.49
Principal Port: 42186
Principal Hostname: TAHOAD.tahoho.com.tw
Principal Process PID: 872
Target Administrative Domain: TAHOHO.COM.TW
Target User ID: 950491
Target Windows SID: S-1-5-21-845223939-707100287-312552118-20227

帳號 950491 登入帳號驗證時 使用 RC4 加密的票據授予服務 (TGS) 請求
此為正常登入行為.

("使用 RC4 加密的票據授予服務" 係因 AD 缺失改善調整導致,尚在調整修正中)

#2 - 2026-01-12 13:07 - Joy Liao

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202512011150-nwp9q.png	46.6 KB	2025-12-01	益利 周