

02\_資安事件及異常紀錄 - 一般 #1098

INCGC-8691-Windows Brute Force Attempt Detected Logon Type 3

2025-11-10 17:46 - Joy Liao

|       |           |        |         |
|-------|-----------|--------|---------|
| 狀態:   | Closed-關閉 | 開始日期:  |         |
| 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 - 2025-11-28 18:09 - 益利 周
- 檔案 clipboard-202511281810-epzsd.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

**Asset Owner :** TWBU  
**Priority:** Medium  
**Description:**

Start Time: 2025-08-28 15:22:00 TST  
End Time: 2025-08-28 15:32:00 TST  
Rule Name: Windows\_Brute\_Force\_Attempt\_Detected\_Logon\_Type\_3  
Rule Description: Logon Type 3 Bruteforce  
Risk Score: 90  
Log Type: WINEVTLOG  
Event Type: USER\_LOGIN  
Vendor Name: Microsoft  
Product Name: Microsoft-Windows-Security-Auditing  
Product Event Type: 4625  
Product Log ID: 162191986  
Opcode: 0  
Channel: Security  
Device: [AzureFlexSRV.tahoho.com.tw](#)  
Principal Hostname: [AzureFlexSRV.tahoho.com.tw](#)  
Principal Windows SID: S-1-0-0  
Principal Subject Logon ID: 0x0  
Principal Process PID: 0x0  
Target Administrative Domain: TAHOHO  
Target User ID: 870742  
Target Windows SID: S-1-0-0  
Target Process File Full Path: NtLmSsp

員工編號 870742 密碼錯誤

- #2 - 2026-01-12 13:07 - Joy Liao
- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

|                                  |         |            |      |
|----------------------------------|---------|------------|------|
| clipboard-202511281810-epzsd.png | 35.8 KB | 2025-11-28 | 益利 周 |
|----------------------------------|---------|------------|------|