

02_資安事件及異常紀錄 - 一般 #1123

INCGC-13563-Windows Scheduled Task Created

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 15:59 - 益利 周
- 檔案 clipboard-202511281558-6bpjz.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: Low

Description:

Start Time: 2025-10-23 23:07:43 TST

End Time: 2025-10-23 23:07:43 TST

Rule Name: windows_scheduled_task_created

Priority: Low

Risk Score: 20

Log Type: WINEVTLOG

Event Type: SCHEDULED_TASK_CREATION

Vendor Name: Microsoft

Product Name: Microsoft-Windows-Security-Auditing

Product Event Type: 4698

Product Log ID: 63177327

Opcode: 0

Channel: Security

Device: [AWSUS.tahoho.com.tw](#)

Principal Hostname: [AWSUS.tahoho.com.tw](#)

Principal Administrative Domain: TAHOHO

Principal User ID: AWSUS\$

Principal Windows SID: S-1-5-18

Principal Subject Logon ID: 0x3e7

Principal Process File Full Path: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25090.3009-0\MpCmdRun.exe

Principal Process PID: 3148

Mitre Tactic: Persistence

Mitre Technique: Scheduled Task/Job

系統自動排程

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

檔案

clipboard-202511281558-6bpjz.png	47.2 KB	2025-11-28	益利 周
----------------------------------	---------	------------	------