TLP:AMBER

資安事件單填寫指南

臺灣學術網路危機處理中心團隊(TACERT)製

2025 年 11 月 V1 版

一、 前言

為確保各校資安事件通報內容正確且具可追溯性，本文件以實際範例說明事件單之填寫重點，並列出常見錯誤作法作為反面案例，協助各校資安事件單填寫人員瞭解正確紀錄方式，提升通報品質與應變效率。

二、 正反面填寫範例

範例來源為 ASOC 開立之系統被入侵事件單。

1、 正面案例內容舉例

(1). 事件主旨(開單單位提供之情資)

教育部資安通告-國立某大學[140.XXX.224.0]OpenSSH 競爭條件漏洞(NASOC-Rule OpenSSH Vulnerability Risk (CVE-2024-6387)。

(2). 事件描述(開單單位提供之情資)

CVE-2024-6387 為 OpenSSH 訊號處理程序的競爭條件漏洞，允許駭客在不需要身分驗證的情況下，自遠端執行任意程式。此漏洞在 64 位元系統中不易觸發，但還是會有邏輯上的風險，請盡速更新安全版本或實施緩解措施。

(3). 調查說明

使用者設備遭外部測試發現有 OPENSSH 漏洞。

(4). 破壞程度

目前尚未發現有遭破壞跡象。

(5). 事件說明

老師研究電腦(140.XXX.224.60、140.XXX.224.62)遭外部測試發現有OPENSSH 漏洞，目前已暫停對外連線。

(6). 影響範圍及損失評估

尚無。

(7). 解決辦法

中斷受害主機網路連線行為至主機無安全性疑慮。

2、 反面案例內容舉例

(1). 事件主旨(開單單位提供之情資)

貴單位所屬 IP:120.XXX.XXX.230 疑似對外發送釣魚郵件。

(2). 事件描述(開單單位提供之情資)

本中心接獲外部情資，貴單位 mail server: mail.XXX.edu.tw [120.XXX.XXX.230]上帳號疑似對外發送釣魚郵件，建議盡速確認並解決。

(3). 調查說明

本中心接獲外部情資，貴單位 mail server: mail.XXX.edu.tw [120.XXX.XXX.230]上帳號疑似對外發送釣魚郵件，建議盡速確認並解決。

(4). 破壞程度

待確認。

(5). 事件說明

通知 mail 管理人員處理。

(6). 影響範圍及損失評估

待確認。

(7). 解決辦法

通知 mail 管理人員處理。

3、 正反面對照與填寫重點

為協助各單位更明確掌握事件單的填寫重點，以下整理正反兩種範例之差異，透過實際內容對照，說明在填報過程中常見的疏漏與修正方向。

表 1. 正反面案例對照及重點說明

項目	正面範例	反面範例	填寫重點
調查說明	使用者設備遭外部測試發現有 OPENSSH 漏洞。	本中心接獲外部情資，貴單位 mail server:mail.XXX.edu.tw[120.XXX.XXX.230]上帳號疑似對外發送釣魚郵件，建議盡速確認並解決。	需填寫實際初步調查結果，請勿複製原情資內容。
破壞程度	目前尚未發現有遭破壞跡象。	待確認。	若無受害跡象可填寫「無」；若有，請明確列出受影響範圍與狀況。「待確認」、「清查中」等詞彙無法反映實際狀況，若填寫，需額外以 EMAIL 補件說明。
事件說明	老師研究電腦(140.XXX.224.60、140.XXX.224.62)遭外部測試發現有 OPENSSH 漏洞，目前已暫停對外連線。	通知 mail 管理人員處理。	此反面案例沒有寫出實際如何處理，請寫出已完成的具體處理行動，若尚在處理中，請說明目前進度與預計完成時間。

項目	正面範例	反面範例	填寫重點
影響範圍及損失評估	尚無。	待確認。	應以事實為主，並非可能造成的傷害。若有明確受害跡象，請填寫實際影響範圍。「待確認」、「清查中」等詞彙無法反映實際狀況，若填寫，需額外以 EMAIL 補件說明。
解決辦法	中斷受害主機網路連線行為至主機無安全性疑慮。	通知 mail 管理人員處理。	此反面案例沒有寫出實際如何處理，需填寫針對此情資最終的解決辦法。

三、 填寫原則與常見錯誤

資安事件單請據實填寫並避免以下常見錯誤。

1. 請勿使用「待確認」、「清查中」、「未知」、「無」等不確定性描述，這些詞彙無法反映實際處理狀況，應以實際調查結果或目前處理狀況填報。若填寫，需額外以 EMAIL 寄至本中心(service@cert.tanet.edu.tw)補件說明，交由本中心協助修改事件單內容。
2. 請勿直接複製貼上情資或簡訊原文，情資非處理結果，需有實際處置說明。若填寫，須以 EMAIL 補件說明並由本中心協助修改事件單內容。
3. 若實際狀況無受害跡象，可於「破壞程度」及「影響範圍及損失評估」填寫為「無」，無須填寫可能造成的傷害，此事件單將為事件等級 0 之情資。若有明確受害跡象，請填寫實際影響範圍，並選擇適當影響等級。
4. 關於「調查說明」、「事件說明」，請填寫已完成的具體處理行動，例：已修補系統漏洞並重新掃描確認無異常。若尚在處理中，請說明目前進度與預計完成時間，例：已通知廠商排定 5/10 修補，預計 5/12 完成。

四、 結語

通報資安事件不僅為法定程序，更為後續資安評估及風險分析的重要依據。請各單位確實記錄調查過程與修補情形，以建立可追蹤、可考證的資安處理紀錄。良好的填報品質可大幅減少後續追查與補件，也能展現學校對資安管理的重視與專業度。