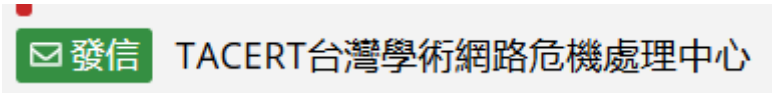
TACERT 資安窗口常見問題

- 密碼變更、重設失敗：
  TACERT 會進後台人工重設密碼，連同 OID 一起寄信回覆。
  校方須提供完整校名或 OID，以及 Email，使得 TACERT 查詢、重設密碼與提供資訊給對方。
  「請提供本中心貴單位全名/OID，以及 Email，謝謝您。」

- 事件單等級、內容調整：
  因送出後學校無法調整內容，由 TACERT 依照要求進後台調整。
  「請提供本中心欲調整之事件單編號，以及欲調整之內容，謝謝您。」

- 事件單錯誤重派、刪除問題：
  TACERT 進後台重新輸入正確 OID 並重派，或是把工單刪除。
  「請提供本中心錯誤事件單之編號，以及有問題之內容，謝謝您。」

- HITCON 修補回報：
  學校方告知漏洞編號，並由 TACERT 進入 HITCON 後台更改漏洞狀態。
  「請確認 HITCON 之漏洞詳情頁面，若該漏洞上方發信單位為 TACERT 台灣學術網路危機處理中心，即可由本中心調整漏洞狀態為已修補，再請提供本中心 HITCON 漏洞編號，謝謝您。」



- HITCON 帳號遺失、申請組織帳號問題：
  HITCON 將漏洞所屬權派給校方，因帳號遺失或沒有組織帳號，無法自行更改，會由本中心寄信通知 HITCON 修改漏洞狀態，或是請學校申請一個組織帳號並驗證，通過後自行更改漏洞狀態。討論過後可請學校自行通知 HITCON，或是將 HITCON 聯繫方式告訴校方。
  「由於HITCON 官方會優先將漏洞權限派發給有 HITCON 平台帳號的單位，因此本中心無法更改漏洞的狀態，也無法從後台查詢到此漏洞，需使用貴單位的 HITCON 帳號，才有權限將漏洞狀態更改為已修補。因此有以下建議方式：
  1. 重新創辦貴單位之 HITCON 帳號，並申請組織帳號，申請組織帳號後可自行新增或移除共同管理組織帳號的使用者，並獲得後台權限(可被派發漏洞資訊及更改漏洞狀態)，若申請途中有遇到問題，可寄信至 service@zeroday.hitcon.org，請官方幫忙協調。

2. 將漏洞修補完成後，通知本中心，由本中心向 HITCON 寄信，請官方更改漏洞狀態。由於 HITCON 需閱讀信件，此方案可能需要幾天時間才能將漏洞狀態更改。謝謝您。」

- 通報流程、填寫問題：

知悉後，一小時內進行通報。當收到資安情資後，經適當且有效的系統調查後，並未發現有直接或間接證據可證明系統遭受到資安事件之威脅即可選擇 INFO(資安情資)。建議在進行系統調查時進行下列步驟：

(1) 檢查系統或網路相關 LOG 資訊，查看是否有異常之處。
(2) 利用如 TCPVIEW 工具軟體或 netstat 指令來查看系統是否有開啟可疑之服務或是否有可疑之來源連線。
(3) 查看防火牆之連線記錄，確認是否有可疑之連線。
(4) 如果有設置入侵偵測軟體（IDS），進行查看是否有惡意的連線行為。

事件通報應變時效因級數而有所不同，「1」、「2」級事件需於 72 小時內完成；「3」、「4」級事件需於 36 小時內完成。

「情資類型」：此資訊為事件原始情資來源之資訊類型，共可分為下列 10 項類型，請選擇適當之類型。

(1). 惡意內容：針對透過文字、照片、影片等形式散播不當內容之事件。
(2). 惡意程式：針對與相關惡意程式之事件。
(3). 資訊蒐集：針對透過掃描、探測及社交工程等攻擊手法取得資訊之事件。
(4). 入侵嘗試：針對嘗試入侵未經授權主機之事件。
(5). 入侵攻擊：針對系統遭未經授權存取或取得系統/使用者權限之事件。
(6). 阻斷服務：針對影響服務可用性或造成服務中斷之攻擊事件。
(7). 資訊內容安全：針對系統遭未經驗證存取或影響資訊機敏性之事件。
(8). 詐欺攻擊：針對偽冒他人身分、系統服務及組織等進行攻擊行為之事件。
(9). 系統弱點：針對系統存在弱點之事件。

應變流程之「損害控制狀態」可分為完成下列兩種狀態，請依實際狀況選擇適合的選項：
(1) 損害控制：已控管此事件所造成的危害。
(2) 完成損害控制與復原：已控管此事件所造成的危害並已完成系統復原。

改善措施欄位：改善措施指各連線單位於完成通報應變後，針對事件發生提出相關改善措施，以完備事件處理流程及預防事件重覆發生。

- 通報演練流程、填寫問題：
  第一、第二聯絡人需在演練資料整備作業期間更換一次密碼，並檢查資安聯絡人資料是否正確。演練以「告知通報」形式進行，通報演練作業期間以郵件及簡訊傳送「資安演練事件通知單」，演練模擬事件通知簡訊及郵件上皆加註「告知通報演練」字樣，另事件單編號皆以「DRILL」開頭進行編碼。

  執行演練單位於收到 mail 及簡訊通知後，應於規定的時限內至教育機構資安通報演練平台完成事件通報流程，並依事件等級於處理時限內完成事件應變處理並結案。通報與填寫方式與正式事件單相同。
  演練平台網址：https://drill.cert.tanet.edu.tw

- 佐證資料申請：
  確認事件單的「發佈編號」後，可至「事件附檔下載」，下載所需之 LOG 附檔。

- 通報平台聯絡人異動、新增及刪除問題：
  聯絡人若已不在職，可先申請重設密碼後請他人登入，並修改個人資料，以更換新的聯絡人；若在職，可直接請異動之聯絡人修改個人資料。要新增或是刪除聯絡人，必須使用第一或第二聯絡人帳號，在帳號管理裡面做新增或是刪除後面聯絡人的帳號。

- EWA 事件單填寫問題：
  處理狀況分為四種。
  1. 確實事件：經查證後為確實事件，須先「自行通報」，並填入自行通報的資安事件編號。
  2. 確實事件(未造成損害)：一樣須通報後填入資安事件單編號。
  3. 誤判：經查證後確認為誤判事件，並於「原因」欄位中，說明誤判原因。
  4. 無法判斷：經查證後確認為無法判斷事件，於「原因」欄位中，說明無法判斷原因。