◎第一線人員	
機關名稱	國立中央大學附屬中壢高級中學
資安聯絡人	黃憲銘
EMAIL	mozart@clhs.tyc.edu.tw
聯絡電話	03-493-2181
分機	63

◎區縣市網人員	
機關名稱	桃園區域網路中心
資安聯絡人	呂芳發
聯絡電話	03-422-7151#57512
E-mail	tanet_ncu@cc.ncu.edu.tw

詳細資料			
發佈編號	DRILL-DEF-2024-364	**發佈時間**	2024-09-02 10:15:49
事件類型	惡意網頁	**發現時間**	2024-09-02 10:15:49
事件主旨	資安事件通告─貴單位[國立中央大學附屬中壢高級中學]]網站內網站被置入詐騙網頁		
事件描述	TACERT 接獲外部情資，貴單位遭檢舉該主機網站有偽造的詐騙網頁(網址如下:https://xxx.xxx.xxx.xxx/xxxx.html)，用來誘騙一般使用者連線至惡意的釣魚網站。		
手法研判	由於該主機內之網頁應用程式有提供上傳功能，但該功能並未設置適當的權限控管，因此可能藉由此管道上傳惡意網頁。		
處理建議	建議立即採取下列步驟：1. 請立即移除該詐騙網頁檔案 2. 檢查該網站具有上傳功能之網頁程式的權限控管是否正確。		

參考資料	無

1. 通報型態：	
告知通報編號：	DRILL-DEF-2024-364
2. 事件發生時間：	2024-09-02 10:15:49
3. 確認(知悉)為資安事件時間：	2024-09-02 10:18:14
4. 設備資料：	
ＩＰ位置：	120.114.22.33
網際網路位置：	https://www.xxx.edu.tw/cba.index
設備廠牌、機型：	華碩 TS100 E6
作業系統：	Centos Linux 5.4
受駭應用軟體：	sendmail server
已裝置之安全防護軟體：	
	防毒軟體：Avira 10.0.0.561 防火牆：iptables IPS/IDS：snort 2.8.3 其它：無
受駭設備類型：	大型主機(Mainframe)-

受害設備說明：	網站主機
損害類別說明：	資料外洩-
攻擊手法：	社交工程
調查說明：	由於該主機內之網頁應用程式有提供上傳功能，但該功能並未設置適當的權限控管，因此可能藉由此管道上傳惡意網頁。
情資類型：	N/A
資安事件損害控制：	是：完成損害控制

5. 資通安全事件：基本資料

事件分類：	DEF-惡意網頁-
破壞程度：	由於該主機內之網頁應用程式有提供上傳功能，但該功能並未設置適當的權限控管，因此可能藉由此管道上傳惡意網頁。
事件說明：	由於該主機內之網頁應用程式有提供上傳功能，但該功能並未設置適當的權限控管，因此可能藉由此管道上傳惡意網頁。

6. 資通安全事件：影響等級及說明

資安事件判斷：

(1) 機密性衝擊 -1 級-非核心業務資訊遭輕微洩漏

(2) 完整性衝擊 -1 級-非核心業務資訊或非核心資通系統遭輕微竄改

(3) 可用性衝擊- 1 級-非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響

資安事件綜合評估等級：1 級

影響範圍及損失評估

可能有一般使用者連線至惡意的釣魚網站。

7. 是否需要支援? 否

8. 通報完成時間： 2024-09-02 10:27:24

9. 通報事件單編號： 364

◎緊急應變措施：

已停止伺服器之服務，待處理完成後再上線

解決辦法：

1. 請立即移除該詐騙網頁檔案 2. 檢查該網站具有上傳功能之網頁程式的權限控管是否正確。

解決時間： 2024-09-02 10:23:57

◎改善措施：

改善辦法：

依資通安全相關管理規範進行改善措施

改善時間： 2024-09-05 10:20:14

通報演練分數	應變演練分數	資料正確率分數
2	2	2

◎區縣市網通報審核

通報審核結果:通過

區縣市網審核時間:2024-09-02 10:28:39

◎區縣市網應變審核

區縣市網應變審核結果:通過

區縣市網應變審核時間:2024-09-02 10:28:39

◎資安通報應變小組通報審核

資安通報應變小組審核結果:未審核

資安通報應變小組審核時間:

◎資安通報應變小組應變審核

資安通報應變小組應變審核結果:無需審核

資安通報應變小組應變審核時間: