友善列印

◎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	TACERT-105-202405-301-00093	**發佈時間**	2024-05-15 15:00:13
事件類型	威脅情報	**發現時間**	2024-05-15 14:31:53
事件主旨	[HITCON ZeroDay] 資安通報-國立中央大學附屬中壢高級中學[203.68.92.34] 網站存在任意檔案上傳(Arbitrary File Upload)漏洞		
事件描述	[HITCON ZeroDay漏洞編號: ZD-2024-00143] TACERT 接獲HITCON ZeroDay團隊通知，發現貴單位[203.68.92.34]網站存在任意檔案上傳(Arbitrary File Upload)漏洞，攻擊者可上傳任意檔案至該主機，有機會經由上傳之文件取得該主機系統權限，煩請協助處理。 問題網址：http://www.clhs.tyc.edu.tw/ 問題網頁:upload_file.php。 有關本案的詳細資訊請參考「事件附檔」。		
手法研判			
處理建議	1.攻擊者可能上傳並執行惡意程式碼，建議盡快修補。2.建議進行權限控管，移除不必要之網頁。3.本案為通用型漏洞，煩請處理完畢後將處理結果(附上事件單編號)回覆至教育機構資安通報應變小組服務信箱 (service@cert.tanet.edu.tw) ，以利彙整資訊向HITCON ZeroDay團隊申請處理狀態更新。4.佐證資料已隨事件單匯入教育機構資安通報平台，煩請登入後於左側「事件附檔下載」中於此事件右側「下載」功能即可下載佐證資料。		
參考資料			

1. 通報型態：	**告知通報**
告知通報編號：	TACERT-105-202405-301-00093
2. 事件發生時間：	2024-05-15 14:31:53
3. 確認(知悉)為資安事件時間：	2024-05-15 15:12:43

4. 設備資料：	
ＩＰ位置：	203.68.92.34
網際網路位置：	https://www.clhs.tyc.edu.tw
設備廠牌、機型：	
作業系統：	CentOS 7
受駭應用軟體：	
已裝置之安全防護軟體：	
	防毒軟體：無 防火牆：無 IPS/IDS：無 其它：無
受駭設備類型：	個人電腦
受害設備說明：	
損害類別說明：	
攻擊手法：	社交工程
調查說明：	
情資類型：	惡意內容
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：	INFO-威脅情報-
破壞程度：	已接獲維護廠商數位果子通知，該漏洞已於昨晚緊急修補完成。 目前並無系統或設備受影響。
事件說明：	已接獲維護廠商數位果子通知，該漏洞已於昨晚緊急修補完成。 目前並無系統或設備受影響。
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 -0級-無系統或設備受影響	
(2) 完整性衝擊 -0級-無系統或設備受影響	
(3) 可用性衝擊- 0級-無系統或設備受影響	

資安事件綜合評估等級：情資	
影響範圍及損失評估	
已接獲維護廠商數位果子通知，該漏洞已於昨晚緊急修補完成。目前並無系統或設備受影響。	
7. 是否需要支援?	否
8. 通報完成時間：	2024-05-15 15:24:46
9. 通報事件單編號：	211027

◎緊急應變措施：
直接處理完成，解決辦法詳見【解決辦法】
解決辦法：
已接獲維護廠商數位果子通知，該漏洞已於昨晚緊急修補完成。目前並無系統或設備受影響。
解決時間： 2024-05-15 15:24:18
◎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： 2024-05-18 15:13:43

承辦人：	**單位主管：**	**資安長官：**