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-105-202411-00000040	**發佈時間**	2024-11-26 15:30:13
事件類型	情資	**發現時間**	2024-11-26 15:11:40
事件主旨	[HITCON ZeroDay] 資安通報 - 國立中央大學附屬中壢高級中學[203.72.181.125] 存在 阻斷服務（DoS） 漏洞		
事件描述	[HITCON ZeroDay漏洞編號: ZD-2024-01482] TACERT 接獲HITCON ZeroDay團隊通知，發現貴單位系統[203.72.181.125]存在阻斷服務（DoS） 漏洞，攻擊者可利用此漏洞造成系統服務阻斷，煩請協助處理。問題網址：http://moodle.clhs.tyc.edu.tw		
手法研判			
處理建議	1.此漏洞可能導致攻擊者可利用此漏洞造成系統服務阻斷，建議盡快修補。 2.有關本案詳細資訊請至HITCONZeroDay漏洞平台瀏覽。 3.煩請務必下載佐證資料，並於處理完畢後將處理結果回覆至資安通報應變小組信箱 (service@cert.tanet.edu.tw) ，以利進行事件複檢及狀態更新。		
參考資料			

1. 通報型態：	**告知通報**
告知通報編號：	TACERT-105-202411-00000040
2. 事件發生時間：	2024-11-26 15:11:40
3. 確認(知悉)為資安事件時間：	2024-11-26 17:23:31
4. 設備資料：	
ＩＰ位置：	203.72.181.125

網際網路位置：	
設備廠牌、機型：	
作業系統：	Windows
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：	系統存在阻斷服務（DoS） 漏洞，攻擊者可利用此漏洞造成系統服務阻斷。
損害類別說明：	other 無任何損害。
攻擊手法：	弱密碼/密碼遭暴力破解
調查說明：	[HITCON ZeroDay漏洞編號: ZD-2024-01482] TACERT 接獲HITCON ZeroDay 團隊通知，發現貴單位系統[203.72.181.125]存在阻斷服務（DoS） 漏洞，攻擊者可利用此漏洞造成系統服務阻斷，煩請協助處理。
情資類型：	其他
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-情資-
破壞程度：	無任何破壞。
事件說明：	馬上聯繫權責單位，請權責單位即刻更改密碼，並告知密碼規則需要有英文大寫、小寫、數字及特殊符號至少12碼以上。
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	
無任何損失。	
7. 是否需要支援?	否
8. 通報完成時間：	2024-11-26 17:39:24
9. 通報事件單編號：	213212

◎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：
馬上聯繫權責單位，請權責單位即刻更改密碼，並告知密碼規則需要有英文大寫、小寫、數字及特殊符號至少12碼以上。
解決時間： 2024-11-26 17:39:00
◎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： 2024-11-29 17:24:31

承辦人：	**單位主管：**	**資安長官：**