

## ANA事件單通知:TACERT-ANA-2025063008060808【漏洞預警】杭特電子混合式監視系統主機存在2個重大資安漏洞

教育機構ANA通報平台

發佈編號	TACERT-ANA-2025063008060808	發佈時間	2025-06-30 08:49:08
事故類型	ANA-漏洞預警	發現時間	2025-06-30 08:49:08
影響等級	低		

[主旨說明:]【漏洞預警】杭特電子混合式監視系統主機存在2個重大資安漏洞

[內容說明:]

轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202506-00000017

【杭特電子 混合式監視系統主機 - Exposure of Sensitive System Information】(CVE-2025-6561, CVSS : 9.8) 杭特電子部分混合式監視系統主機型號(HBF-09KD與HBF-16NK)存在Exposure of Sensitive Information漏洞, 未經身分鑑別之遠端攻擊者可直接存取系統設定檔案取得管理者明文帳號密碼。

【杭特電子 混合式監視系統主機 - OS Command Injection】(CVE-2025-6562, CVSS : 8.8) 杭特電子部分混合式監視系統主機型號(HBF-09KD與HBF-16NK)存在OS Command Injection漏洞, 允許已取得一般權限之遠端攻擊者注入任意作業系統指令並於設備上執行。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」, 煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

- HBF-09KD、HBF-16NK
- V3.1.67\_1786 BB11115(含)以前版本

[建議措施:]

更新韌體版本至V31.70\_1806 BB50604(含)以後版本

[參考資料:]

1. 杭特電子 混合式監視系統主機 - Exposure of Sensitive System Information

<https://www.twcert.org.tw/tw/cp-132-10199-9c5c6-1.html>

2. 杭特電子 混合式監視系統主機 - OS Command Injection

<https://www.twcert.org.tw/tw/cp-132-10201-044e9-1.html>

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：[service@cert.tanet.edu.tw](mailto:service@cert.tanet.edu.tw)