教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026062208060808	發佈時間	2026-06-22 08:54:08
事故類型	ANA-漏洞預警	發現時間	2026-06-22 08:54:08
影響等級	低		

[主旨說明:]【漏洞預警】Fortinet 防火牆等設備遭受憑證竊取攻擊，請儘速確認並修補

[內容說明:]

轉發　國家資安資訊分享與分析中心 資安訊息警訊 NISAC-400-202606-00000006

研究人員發現有攻擊者針對 Fortinet 防火牆與 VPN 裝置等設備進行大規模憑證竊取攻擊，且疑似掌握相關設備之帳密資料，進而大規模破解相關設備防護措施。

請機關運用下列查詢工具確認自身設備是否已遭揭露，並請盡速採取改善措施。 工具連結：https://www.hudsonrock.com/fortinet

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:]

所有 Fortinet 設備

[建議措施:]

1.隱藏管理介面：盡速確認設備管理介面是否暴露於網際網路，並將管理介面從公開網際網路移除，僅允許受信任的 IP 或透過跳板機/VPN 方式存取。

2.全面重置設備密碼：立即更換所有 Fortinet 設備管理介面與 VPN 之管理者密碼。

3.啟用多因子驗證機制（MFA）：建議在所有遠端存取與管理員帳戶啟用多因素認證。

4.強制升級雜湊演算法：升級 FortiOS 後，要求所有管理員至少登入一次防火牆，系統會自動將密碼加密方式升級為更難被破解的 PBKDF2 演算法。

[參考資料:]

1. https://www.hudsonrock.com/fortinet