

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026070604072222	發佈時間	2026-07-06 16:27:23
事故類型	ANA-漏洞預警	發現時間	2026-07-06 16:27:23
影響等級	低		

[主旨說明:] **【漏洞預警】 WatchGuard Firebox 存在重大資安漏洞(CVE-2026-13368)**

[內容說明:]

轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202607-00000002

WatchGuard Firebox 是一款次世代防火牆產品，提供多層次防護，包括防毒、IPS、APT 阻擋及垃圾郵件過濾。近日 WatchGuard 發布重大資安漏洞公告(CVE-2026-13368，CVSS 4.x：9.2)，該漏洞源於 Mobile User VPN with IKEv2 的 LDAP 驗證機制存在競爭條件（Race Condition），進而造成釋放後使用（Use-After-Free）漏洞。

若 Firebox 已設定 Mobile User VPN with IKEv2 並使用外部 LDAP 驗證伺服器，未經身分驗證的遠端攻擊者可利用此漏洞，以 iked 進程的上下文中執行任意程式碼。

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:]

Fireware OS 2025.1 版本

Fireware OS 12.x 版本

Fireware OS 12.5.x (T15&T13) 版本

Fireware OS 11.x 版本

[建議措施:]

請更新至以下版本：Fireware OS 2026.2.1 版本、Fireware OS 12.12.1 版本

[參考資料:]

1. <https://www.twcert.org.tw/tw/cp-169-11022-eee7d-1.html>