教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026110409112929	發佈時間	2026-11-04 09:53:30
事故類型	ANA-漏洞預警	發現時間	2026-11-04 09:53:30
影響等級	中		

[主旨說明:]【漏洞預警】WatchGuard Fireware OS 存在 2 項高風險安全漏洞(CVE-2026-112709 與 CVE-2026-112710)，請儘速確認並進行處置

[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-200-202611-00000001

研究人員發現 WatchGuard Fireware OS 存在 2 項堆積型緩衝區溢位(Heap-based Buffer Overflow)漏洞(CVE-2026-112709 與 CVE-2026-112710)，當 Firebox 設備設定為 Active Directory 身分鑑別伺服器時，未經身分鑑別之遠端攻擊者可透過控制或攔截該伺服器之流量，並藉由特製回應觸發漏洞，進而導致阻斷服務或執行任意程式碼，請儘速確認並進行處置。

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 至 2026.4(不含)版本

Fireware OS(Firebox T15 與 T35 以外機型)12.0 至 12.12.4(不含)版本

Fireware OS(Firebox T15 與 T35)12.0 至 12.5.22(不含)版本
[建議措施:] 官方已針對漏洞釋出修補或更新，請參考官方說明進行處置，網址如下： https://psirt.watchguard.com/CVE-2026-112709 https://psirt.watchguard.com/CVE-2026-112710
[參考資料:] 1. https://nvd.nist.gov/vuln/detail/CVE-2026-112709 2. https://nvd.nist.gov/vuln/detail/CVE-2026-112710 3. https://psirt.watchguard.com/CVE-2026-112709 4. https://psirt.watchguard.com/CVE-2026-112710