

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026102702104747	發佈時間	2026-10-27 14:07:48
事故類型	ANA-漏洞預警	發現時間	2026-10-27 14:07:48
影響等級	中		

[主旨說明:] **【漏洞預警】Fortinet 多款資安產品釋出安全強化更新，請儘速確認並完成更新**

[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-200-202610-00000025

網路安全設備廠商 Fortinet 預定於 115 年 10 月 22 日發布多款產品安全強化更新，涵蓋 FortiOS、FortiManager、FortiAnalyzer、FortiMail 及 FortiAuthenticator 等 5 大系列，包含重大及高風險漏洞修補。為降低資安風險，請各單位儘速盤點所使用之相關產品及版本，優先更新對外連網設備，以維護機關資通安全。

Fortinet 表示，本次漏洞係透過 AI 輔助安全測試計畫所發現，相關漏洞技術細節預計於 115 年 11 月 10 日公布。考量漏洞細節公開後可能增加遭攻擊風險，請各單位及早完成更新準備，並於修補版本發布後儘速辦理升級。 [更新資訊] 更新對象： 使用 FortiOS、FortiManager、FortiAnalyzer、FortiMail 及 FortiAuthenticator 等產品之機關。 更新版本： FortiOS：8.0.2、7.6.8、7.4.13、7.2.14 或以上版本。 FortiManager：8.0.2、7.6.8、7.4.12、7.2.13 或以上版本。 FortiAnalyzer：8.0.2、7.6.8、7.4.12、7.2.13 或以上版本。 FortiMail：8.0.2、7.6.7、7.4.9 或以上版本；使用 7.2 分支者，應升級至 7.4 或以上分支。 FortiAuthenticator：8.0.4、6.6.11 或以上版本。

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:]

FortiOS 7.2.0–7.2.13、7.4.0–7.4.12、7.6.0–7.6.7、8.0.0–8.0.1

FortiManager 7.2.0–7.2.12、7.4.0–7.4.11、7.6.0–7.6.7、8.0.0–8.0.1

FortiAnalyzer 7.2.0–7.2.12、7.4.0–7.4.11、7.6.0–7.6.7、8.0.0–8.0.1

FortiMail 7.2.0–7.2.9、7.4.0–7.4.8、7.6.0–7.6.6、8.0.0–8.0.1

FortiAuthenticator 6.6.0–6.6.10、8.0.0–8.0.3

[建議措施:]

儘速盤點相關設備及軟體版本，優先處理對外連網設備。依原廠建議完成更新，更新前應先備份設定，並確認更新後設備運作正常。如暫時無法更新，應限制管理介面對網際網路之存取，僅允許可信任 IP 連線；必要時採取網路隔離或其他適當防護措施，以降低遭受攻擊之風險。

[參考資料:]

1. https://www.fortinet.com/blog/ciso-collective/fortinet-releases-security-hardening-release-for-multiple-products?utm_