教育機構 ANA 通報平台

發佈編號	TACERT-ANA-20250626020603O3	發佈時間	2025-06-26 14:55:04
事故類型	ANA-漏洞預警	發現時間	2025-06-26 14:55:04
影響等級	中		

[主旨說明:]【漏洞預警】Cisco 近日發布更新以解決 Meraki MX 的安全性弱點，建議請管理者儘速評估更新！

[內容說明:]

轉發 中華資安 CHTSECURITY-200-202506-00000001

CVE-2025-20271 : CVSS 8.6 未經身份驗證的遠端攻擊者可以透過向受影響的設備發送精心製作的 HTTPS 請求來利用此弱點。這可能導致 Cisco AnyConnect VPN 伺服器重新啟動，從而造成終止所有現有的 SSL VPN 會話、阻止建立新的 VPN 連線、最終，VPN 服務對合法使用者變得不可用。

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:]

Meraki MX

[建議措施:]

請參考 Cisco 官方網站的說明和處理建議：

1.Meraki MX 韌體 18.107.13 (含)之後的版本 2.Meraki MX 韌體 18.211.6 (含)之後的版本 3.Meraki MX 韌體 19.1.8 (含)之後的版本
[參考資料:] 1. https://nvd.nist.gov/vuln/detail/CVE-2025-20271 2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-sM5GCfm7