國立成功大學 National Cheng Kung University

ANA事件單通知:TACERT-ANA-2026051809053535【漏洞預警】Cisco Catalyst SD-WAN 存在重大資安漏洞(CVE-2026-20182)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2026051809053535	發佈時間	2026-05-18 09:28:36
事故類型	ANA-漏洞預警	發現時間	2026-05-18 09:28:36
影響等級	低		

[主旨說明:]【漏洞預警】Cisco Catalyst SD-WAN 存在重大資安漏洞(CVE-2026-20182)

[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-200-202605-00000011

Cisco Catalyst SD-WAN 是 Cisco 以雲端為中心的軟體定義廣域網路架構，提供集中管理、安全加密及應用效能優化，確保多雲環境的可靠連線，近日Cisco發布重大資安公告。

【CVE-2026-20182，CVSS：10.0】 此漏洞存在於Cisco Catalyst SD-WAN Controller (formerly vSmart) 與 Catalyst SD-WAN Manager (formerly vManage)，允許遠端攻擊者發送特製請求繞過身分驗證，取得內部高權限帳號 (non-root)。

攻擊者後續可利用高權限帳號存取 NETCONF，修改 SD-WAN 網路架構配置，建立惡意網路節點並深入攻擊企業/組織網路。

註：Cisco Catalyst SD-WAN Controller (formerly vSmart) 與 Cisco Catalyst SD-WAN Manager (formerly vManage) 已被發現積極利用於攻擊活動，請儘速採取應變措施。

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:]

Cisco Catalyst SD-WAN On-Prem Deployment、Cisco SD-WAN Cloud-Pro、Cisco SD-WAN Cloud (Cisco Managed)、Cisco SD-WAN for Government (FedRAMP)

[建議措施:]

根據官方網站釋出的解決方式進行修補:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
[參考資料:]

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw