張貼日期：2026/05/19

【漏洞預警】Cisco Catalyst SD-WAN 存在重大資安漏洞(CVE-2026-20182)

- 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。
- 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

計算機與通訊中心
網路系統組 敬啟