

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026080605080707	發佈時間	2026-08-06 17:24:08
事故類型	ANA-漏洞預警	發現時間	2026-08-06 17:24:08
影響等級	低		
[主旨說明:] 【漏洞預警】Cisco Catalyst SD-WAN 存在 4 個重大資安漏洞			
[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-200-202608-00000005 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。Catalyst SD-WAN 軟體開發團隊於內部安全審查期間發現多項安全漏洞，並已完成修補。 目前尚未發現有證據顯示這些漏洞遭到積極利用。為協助客戶及時部署安全更新並簡化漏洞揭露流程，Cisco 已公開相關漏洞資訊及修補建議。 CVE-2026-20303(CVSS：9.9)為輸入驗證不當漏洞；CVE-2026-20304(CVSS：9.9)為存取控制不當漏洞；CVE-2026-20310(CVSS：9.9)為文件存取前連結解析不正確；CVE-2026-20312(CVSS：8.8)為以明文形式儲存敏感資訊。 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 20.9(含)之前版本、 Cisco Catalyst SD-WAN 20.10 版			

本、 Cisco Catalyst SD-WAN 20.11 版本、 Cisco Catalyst SD-WAN 20.12 版本、 Cisco Catalyst SD-WAN 20.13 版本、 Cisco Catalyst SD-WAN 20.14 版本、 Cisco Catalyst SD-WAN 20.15 版本、 Cisco Catalyst SD-WAN 20.16 版本、 Cisco Catalyst SD-WAN 20.18 版本、 Cisco Catalyst SD-WAN 26.1 版本

[建議措施:]

請更新至以下版本： Cisco Catalyst SD-WAN 20.9.10(含)之後版本、 Cisco Catalyst SD-WAN 20.12.8.1(含)之後版本、 Cisco Catalyst SD-WAN 20.15.6(含)之後版本、 Cisco Catalyst SD-WAN 20.18.4(含)之後版本、 Cisco Catalyst SD-WAN 26.1.2(含)之後版本

[參考資料:]

1.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K>

2. <https://nvd.nist.gov/vuln/detail/CVE-2026-20303>

3. <https://nvd.nist.gov/vuln/detail/CVE-2026-20304>

4. <https://nvd.nist.gov/vuln/detail/CVE-2026-20310>

5. <https://nvd.nist.gov/vuln/detail/CVE-2026-20312>