教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2025052109052727	發佈時間	2025-05-21 09:53:27
事故類型	ANA-漏洞預警	發現時間	2025-05-21 09:53:27
影響等級	中		
[主旨說明:] 【漏洞預警】 Cisco IOS XE Software 存在高風險安全漏洞(CVE-2025-20188)，請儘速確認並進行修補			
[內容說明:] 轉發 國家資安資訊分享與分析中心 NISAC-200-202505-00000076 研究人員發現 Cisco IOS XE Software for Wireless LAN Controllers (WLCs)之 Out-of-Band Access Point (AP) Image Download 功能存在任意檔案上傳 (Arbitrary File Upload)漏洞(CVE-2025-20188)，允許未經身分鑑別之遠端攻擊者上傳後門程式以執行任意程式碼。 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」，煩請貴單位協助公告或轉發			
[影響平台:] 影響產品名稱： Cisco IOS XE Software 且開啟 Out-of-Band AP Image Download 功能之設備 影響型號：			

- Catalyst 9800-CL Wireless Controllers for Cloud
- Catalyst 9800 Embedded Wireless Controller (適用於 Catalyst 9300、9400 及 9500 系列交換器)
- Catalyst 9800 系列無線控制器
- Catalyst AP 內嵌式無線控制器

可使用 Cisco Software

Checker(<https://sec.cloudapps.cisco.com/security/center/softwarechecker.x>)
確認現行使用之 Cisco IOS XE Software 版本是否受到影響。

[建議措施:]

1.官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC>

2.若暫時無法更新，請先行關閉 Out-of-Band AP Image Download 功能以避免遭到攻擊利用。

[參考資料:]

1.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC>

2. <https://netmag.tw/2025/05/13/cisco-ios-xe-wireless-controller-vulnerability>