張貼日期：2025/05/22

【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

- 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。
- 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. 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. 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

---

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20250522_04

Last update: **2025/05/22 15:18**