張貼日期：2022/04/21

【資安漏洞預警Cisco多款無線網路控制器軟體存在安全漏洞(CVE-2022-20695)請儘速確認並進行更新！

- 主旨說明Cisco多款無線網路控制器軟體存在安全漏洞(CVE-2022-20695)允許攻擊者繞過身分鑑別取得裝置控制權，請儘速確認並進行更新！

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202204-0641
  - 研究人員發現Cisco多款無線網路控制器(Wireless LAN Controller簡稱WLC)軟體存在安全漏洞(CVE-2022-20695)肇因於通行碼鑑別演算法實作不當，導致攻擊者可藉由特製之憑證繞過身分鑑別，並以管理權限登入取得裝置控制權。
- 影響平台:
  - 3504 Wireless Controller
  - 5520 Wireless Controller
  - 8540 Wireless Controller
  - Mobility Express
  - Virtual Wireless Controller(vWLC)
- 建議措施:
  1. 目前Cisco官方已針對此漏洞釋出修復版本，請各機關可聯絡設備維護廠商或參考以下建議進行更新：
     1. 連線至網址：https://software.cisco.com/download/home ，點擊Browse All按鈕。
     2. 選擇Wireless > Wireless LAN Controller > Standalone Controllers
     3. 依所使用之型號下載更新檔。
     4. 使用設備之管理頁面功能更新Cisco WLC軟體至8.10.171.0以後版本。
  2. 若無法更新至最新版本，請參考Cisco官方網頁(https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-auth-bypass-JRNhV4fF)之Workarounds一節，採取緩解措施：
     1. 若環境中不需使用到Mac Filter可透過下列指令重設RADIUS Compatibility mode為預設值config macfilter radius-compat cisco
     2. 若環境中需使用到Mac Filter可透過下列指令調整RADIUS Compatibility mode為cisco或free模式config macfilter radius-compat ciscoconfig macfilter radius-compat free
  3. 透過下列指令可檢查裝置是否受此漏洞影響：
     1. 輸入指令show macfilter summary
     2. 若顯示結果出現RADIUS Compatibility mode為「Other則受此弱點影響。
- 參考資料:
  1. https://www.ithome.com.tw/news/150464
  2. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-auth-bypass-JRNhV4fF
  3. https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/91901-mac-filters-wlcs-config.html

---

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:20220421_03

Last update: **2022/04/21 15:48**