張貼日期：2021/02/17

【資安漏洞預警Cisco 之VPN 路由器存在安全漏洞，請儘速確認並進行更新！

主旨：【資安漏洞預警Cisco 之 VPN 路由器存在安全漏洞 (CVE-2021-1289~CVE-2021-1295等共7個漏洞)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 NISAC-ANA-202102-0566
  - 研究人員發現Cisco中小企業VPN路由器之Web管理介面未正確驗證HTTP請求，導致存在安全漏洞(CVE-2021-1289、CVE-2021-1290、CVE-2021-1291、CVE-2021-1292、CVE-2021-1293、CVE-2021-1294及CVE-2021-1295)、攻擊者可藉由發送特定HTTP封包，進而獲得管理員權限，並可遠端執行任意程式碼。
- 影響平台:
  - 使用1.0.01.02(不含)以前版本之VPN路由器設備如下：
    - RV160 VPN Router
    - RV160W Wireless-AC VPN Router
    - RV260 VPN Router
    - RV260P VPN Router with POE
    - RV260W Wireless-AC VPN Router
- 建議措施: *目前Cisco官方已針對此弱點釋出修復版本，請各機關可聯絡設備維護廠商或參考以下建議進行更新： - 連線至網址：https://software.cisco.com/download/home，點擊Browse All按鈕。 - 按照型號下載更新檔：點擊Routers > Small Business Routers > Small Business RV Series Routers >點選適當的路由器型號 > Wireless Router Firmware選擇1.0.01.02或後續版本進行下載。 - 使用設備之管理頁面功能進行韌體更新 * 參考資料: - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf - https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1289 - https://www.ithome.com.tw/news/142701 - https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1142 —- 計算機與通訊中心 網路系統組 敬啟*