

張貼日期：2022/02/10

【資安漏洞預警】Cisco Small Business RV160、RV260、RV340及RV345系列路由器存在安全漏洞(CVE-2022-20699~20712及CVE-2022-20749)請儘速確認並進行更新！

- 主旨說明：Cisco Small Business RV160、RV260、RV340及RV345系列路由器存在安全漏洞(CVE-2022-20699~20712及CVE-2022-20749)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 國家資安資訊分享與分析中心 NISAC-ANA-202202-0288
 - 研究人員發現Cisco Small Business RV160、RV260、RV340及RV345系列路由器之Web管理介面未正確驗證HTTP請求，導致存在安全漏洞(CVE-2022-20699~20712及CVE-2022-20749)攻擊者可藉由發送特定HTTP封包，進而利用漏洞遠端以管理者權限執行任意程式碼或阻斷服務(DoS)攻擊。
- 影響平台：
 1. 使用韌體1.0.01.05(含)以前版本之下列RV160與RV260系列型號路由器：
 - RV160 VPN Routers
 - RV160W Wireless-AC VPN Routers
 - RV260 VPN Routers
 - RV260P VPN Routers with PoE
 - RV260W Wireless-AC VPN Routers
 2. 使用韌體1.0.03.24版本之下列RV340與RV345系列型號路由器：
 - RV340 Dual WAN Gigabit VPN Routers
 - RV340W Dual WAN Gigabit Wireless-AC VPN Routers
 - RV345 Dual WAN Gigabit VPN Routers
 - RV345P Dual WAN Gigabit POE VPN Routers
- 建議措施：目前Cisco官方已針對這些漏洞釋出修復版本，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. 依所使用之型號下載更新檔：點擊[Routers \ Small Business Routers \ Small Business RV Series Routers \ 點選所使用的路由器型號 \ Small Business Router Firmware]
 1. RV160與RV260系列選擇1.0.01.07或後續版本進行下載。
 2. RV340與RV345系列選擇1.0.03.26或後續版本進行下載。
 3. 使用設備之管理頁面功能進行韌體更新。
- 參考資料：
 1. <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-mult-vuln-KA9PK6D>
 2. <https://www.auscert.org.au/bulletins/ESB-2022.0454>
 3. <https://technews.tw/2022/02/05/cisco-router-vulnerable/>

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:20220210_02



Last update: **2022/02/10 14:57**