

張貼日期：2021/08/10

【資安漏洞預警】Cisco RV340、RV340W、RV345及RV345P Dual WAN Gigabit VPN路由器存在安全漏洞(CVE-2021-1609與1610)，請儘速確認並進行更新！

主旨：【資安漏洞預警】Cisco RV340、RV340W、RV345及RV345P Dual WAN Gigabit VPN路由器存在安全漏洞(CVE-2021-1609與1610)，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 資安訊息警訊 NISAC-ANA-202108-0633
 - 研究人員發現Cisco RV340、RV340W、RV345及RV345P Dual WAN Gigabit 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-2021-1609與1610)，攻擊者可藉由發送特定HTTP封包，進而利用此漏洞遠端執行任意程式碼或阻斷服務(DoS)攻擊。
- 影響平台：
 - 使用韌體1.0.03.22 (不含)以前版本之下列型號路由器：
 - RV340 Dual WAN Gigabit VPN Router
 - RV340W Dual WAN Gigabit Wireless-AC VPN Router
 - RV345 Dual WAN Gigabit VPN Router
 - RV345P Dual WAN Gigabit POE 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：
 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 > 點選適當的路由器型號 > Wireless Router Firmware」選擇1.0.03.22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-rv340-cmdi-nj-rcedos-pY8J3qfy>
 2. <https://www.ithome.com.tw/news/146036>

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/announcement:20210810_02

Last update: **2021/08/10 16:14**

