張貼日期：2019/03/07

[資安漏洞預警通知] Cisco三款VPN路由器產品存在安全漏洞，允許遠端攻擊者執行任意程式碼，請儘速確認並進行修正

主旨：[資安漏洞預警通知] Cisco三款VPN路由器產品存在安全漏洞，允許遠端攻擊者執行任意程式碼，請儘速確認並進行修正

- 內容說明:
  - 研究團隊發現Cisco RV110W、RV130W及RV215W三款VPN路由器產品存在安全性漏洞(CVE-2019-1663)，肇因於此三款產品之網頁管理介面程式未完整驗證用戶提交的資料，導致未經授權的遠端攻擊者可針對目標設備發送特製的HTTP請求，進而造成遠端攻擊者可以管理員權限執行任意程式碼。
- 影響平台:
  - RV110W Wireless-N VPN Firewall，韌體版本1.2.2.1以前的所有版本
  - RV130W Wireless-N Multifunction VPN Router，韌體版本1.0.3.45以前的所有版本
  - RV215W Wireless-N VPN Router，韌體版本1.3.1.1以前的所有版本
- 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. 按照型號下載更新檔：
       1. RV110W Wireless-N VPN Firewall，
          - 點擊「Routers > Small Business Routers > Small Business RV Series Routers > RV110W Wireless-N VPN Firewall > Wireless Router Firmware」選擇1.2.2.1或後續版本進行下載。
       2. RV130W Wireless-N Multifunction VPN Router，
          - 點擊「Routers > Small Business Routers > Small Business RV Series Routers > RV130W Wireless-N Multifunction VPN Router > Small Business Router Firmware」選擇1.0.3.45或後續版本進行下載。
       3. RV215W Wireless-N VPN Router，
          - 點擊「Routers > Small Business Routers > Small Business RV Series Routers > RV215W Wireless-N VPN Router > Wireless Router Firmware」選擇1.3.1.1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-20190227-rmi-cmd-ex
  2. https://www.ithome.com.tw/news/129047

計算機與通訊中心
網路系統組 敬啟