張貼日期：2020/07/15

【資安漏洞預警Juniper SRX系列設備之Junos OS存在安全漏洞，請儘速確認並進行更新

主旨：【資安漏洞預警Juniper SRX系列設備之Junos OS存在安全漏洞(CVE-2020-1647與CVE-2020-1654)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-202007-0565)
  - 研究人員發現Juniper SRX系列設備在有開啟ICAP (Internet Content Adaptation Protocol) Redirect服務的狀態下存在安全漏洞(CVE-2020-1647與CVE-2020-1654)
  - 遠端攻擊者可對目標設備發送特製請求，利用此漏洞進而執行任意程式碼或造成阻斷服務攻擊。
- 影響平台:
  1. 若設備之Junos OS符合以下版本號碼且開啟ICAP Redirect服務，則受CVE-2020-1647影響：
     - 18.1 18.1R3-S9以前版本
     - 18.2 18.2R3-S3以前版本
     - 18.3 18.3R2-S4與18.3R3-S1以前版本
     - 18.4 18.4R2-S5與18.4R3以前版本
     - 19.1 19.1R2以前版本
     - 19.2 19.2R1-S2與19.2R2以前版本
     - 19.3 19.3R2以前版本
  2. 若設備之Junos OS符合以下版本號碼且開啟ICAP Redirect服務，則受CVE-2020-1654影響：
     - 18.1 18.1R3-S9以前版本
     - 18.2 18.2R2-S7與18.2R3-S3以前版本
     - 18.3 18.3R1-S7 18.3R2-S4及18.3R3-S1以前版本
     - 18.4 18.4R1-S7 18.4R2-S4及18.4R3以前版本
     - 19.1 19.1R1-S5 19.1R2以前版本
     - 19.2 19.2R1-S2 19.2R2以前版本
     - 19.3 19.3R2以前版本 * 無序列表項目
- 建議措施:
  目前Juniper官方已針對此弱點釋出更新程式，請各機關聯絡設備維護廠商進行版本確認，並更新Junos OS至下列對應版本：
  1. CVE-2020-1647
     - 18.1 18.1R3-S9
     - 18.2 18.2R3-S3
     - 18.3 18.3R2-S4與18.3R3-S1
     - 18.4 18.4R2-S5與18.4R3
     - 19.1 19.1R2
     - 19.2 19.2R1-S2與19.2R2
     - 19.3 19.3R2
     - 19.4 19.4R1
  2. CVE-2020-1654
     - 18.1 18.1R3-S9
     - 18.2 18.2R2-S7與18.2R3-S3
     - 18.3 18.3R1-S7 18.3R2-S4及18.3R3-S1
     - 18.4 18.4R1-S7 18.4R2-S4及18.4R3

    - 19.1□19.1R1-S5與19.1R2
    - 19.2□19.2R1-S2與19.2R2
    - 19.3□19.3R2
    - 19.4□19.4R1
- 參考資料:
    1. https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11034
    2. https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11031
    3. https://www.ithome.com.tw/news/138793

計算機與通訊中心
網路系統組 敬啟