張貼日期：2024/06/13

【漏洞預警】Check Point VPN Gateway存在高風險安全漏洞(CVE-2024-24919)，請儘速確認並進行修補！

- 主旨說明：Check Point VPN Gateway存在高風險安全漏洞(CVE-2024-24919)，請儘速確認並進行修補！
- 內容說明:
  - 轉發 國家資安資訊分享與分析中心 NISAC-200-202406-00000076，
  - 研究人員發現Check Point VPN Gateway存在路徑遍歷(Path Traversal)漏洞(CVE-2024-24919)，未經身分鑑別之遠端攻擊者可發送偽造請求取得任意系統檔案。該漏洞已遭駭客利用，請儘速確認並進行修補。
    - 影響產品： CloudGuard Network，Quantum Maestro，Quantum Scalable Chassis，Quantum Security Gateways及Quantum Spark Appliances
    - 影響版本：R77.20(EOL)，R77.30(EOL)，R80.10(EOL)，R80.20(EOL)，R80.20.x，R80.20SP(EOL)，R80.30(EOL)，R80.30SP(EOL)，R80.40(EOL)，R81，R81.10，R81.10.x及R81.20
- 影響平台:
  - 影響產品：
    - CloudGuard Network
    - Quantum Maestro
    - Quantum Scalable Chassis
    - Quantum Security Gateways
    - Quantum Spark Appliances
  - 影響版本：
    - R77.20(EOL)
    - R77.30(EOL)
    - R80.10(EOL)
    - R80.20(EOL)
    - R80.20.x
    - R80.20SP(EOL)
    - R80.30(EOL)
    - R80.30SP(EOL)
    - R80.40(EOL)
    - R81
    - R81.10
    - R81.10.x
    - R81.20
- 建議措施:
  - 官方已針對漏洞釋出修補程式，請參考官方說明進行修補，網址如下：https://support.checkpoint.com/results/sk/sk182336
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2024-24919
  2. https://support.checkpoint.com/results/sk/sk182336
  3. https://www.truesec.com/hub/blog/check-point-ssl-vpn-cve-2024-24919-from-an-incident-response-perspective
  4. https://www.greynoise.io/blog/whats-going-on-with-checkpoint-cve-2024-24919

計算機與通訊中心
網路系統組 敬啟