張貼日期：2021/10/04

【資安訊息】 NSA、CISA 分享 VPN 資訊安全小撇步以防禦駭客攻擊

- 主旨說明：【資安訊息】 NSA、CISA 分享 VPN 資訊安全小撇步以防禦駭客攻擊

- 內容說明：
  - 轉發 衛生福利部資安資訊分享與分析中心 資安訊息警訊 HISAC-ANA-202109-0005、
  - 美國網路安全和基礎設施安全局 (CISA) 和國家安全局 (NSA) 發布了加強虛擬專用網路 (VPN) 解決方案。案例分析:
    1. 這兩個機構創建該文件是為了幫助組織提高防禦能力，特別是針對來自國家級駭客過去曾利用 VPN 系統中的漏洞竊取憑證、遠端執行代碼、減弱加密流量、劫持加密流量、並從設備中竊取敏感資料。
    2. 作為加強 VPN 的準則，這兩個機構建議透過以下方式減少伺服器的攻擊面：
       1. 在配置需增強加密和身份驗證。
       2. 在嚴格必要的功能上運作。
       3. 在受保護和監控下對 VPN 存取。
    3. 今年 4 月初，網路安全公司 FireEye 發布了一份報告，在針對美國國防工業基地 (DIB) 的攻擊中使用了Pulse Connect Secure (PCS) VPN 設備中的零時差漏洞。
    4. 大約在同一時間、NSA 和 CISA 警告，為俄羅斯外國情報局 (SVR) 工作的駭客 APT29、Cozy Bear 和 The Dukes 已經成功利用 Fortinet 和 Pulse Secure VPN 設備中的漏洞進行攻擊。
    5. 英國國家網路安全中心 (NCSC) 在 5 月發布一份諮詢報告，將思科和其他網路設備供應商的設備添加到俄羅斯外國情報局 (SVR) 工作的駭客所利用存在的漏洞產品列表中。
    6. 勒索軟體集團也對這種類型的網路存取漏洞表現出極大的興趣，至少利用了 Fortinet、Ivanti (Pulse) 和 SonicWall 的 VPN 解決方案中的漏洞。
    7. Cring、Ragnar Locker、Black Kingdom、 HelloKitty、LockBit、REvil、Conti勒索軟體已成功透過利用 VPN安全漏洞問題破壞了數十家公司。
- 影響平台:無
- 建議措施:無
- 參考資料:https://www.bleepingcomputer.com/news/security/nsa-cisa-share-vpn-security-tips-to-defend-against-hackers-edited/

計算機與通訊中心
網路系統組 敬啟