張貼日期：2020/09/18

【資安攻擊預警】請注意防範國家級駭客組織利用遠端存取設備與微軟Exchange漏洞進行攻擊

主旨：【資安攻擊預警】請注意防範國家級駭客組織利用遠端存取設備與微軟Exchange漏洞進行攻擊

- 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-202009-0585
  - 美國網路安全及基礎設施安全局(CISA)與聯邦調查局(FBI)近期發布國家級駭客組織利用公開之遠端存取設備漏洞與微軟Exchange漏洞對美國政府部門、高科技製造產業、醫療設備、太陽能源領域等進行攻擊。
  - 請檢查所使用之遠端存取設備與微軟Exchange伺服器是否已更新修補，避免遭國家級駭客組織進行漏洞開採利用。
- 影響平台: 遠端存取設備、微軟Exchange伺服器
- 建議措施:
  1. 檢查所列之遠端存取設備與微軟Exchange伺服器上是否有不明帳號、異常登入及異常連線。
  2. 檢查資安防護設備紀錄是否有異常連線。
  3. 依設備原廠與技服中心發布之措施，進行防護設定與與更新修補。
     1. F5 BIG-IP產品存在安全漏洞(CVE-2020-5902與CVE-2020-5903)
        https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1128
     2. Citrix部分產品存在遠端執行程式碼漏洞
        https://www.nccst.nat.gov.tw/VulnerabilityNewsDetail?lang=zh&seq=1448
     3. Pulse Secure數個產品存在多個漏洞
        https://www.nccst.nat.gov.tw/VulnerabilityNewsDetail?lang=zh&seq=1443
     4. 微軟Exchange伺服器存在安全漏洞(CVE-2020-0688)
        https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1117
- 參考資料:
  - https://us-cert.cisa.gov/ncas/alerts/aa20-258a

計算機與通訊中心
網路系統組 敬啟