張貼日期：2020/03/16

【資安漏洞預警】微軟Windows作業系統存在安全漏洞(CVE-2020-0796)□允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

主旨：【資安漏洞預警】微軟Windows作業系統存在安全漏洞(CVE-2020-0796)□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：
  - 轉發國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202003-0324
  - 研究人員發現SMBv3存在安全漏洞(CVE-2020-0796)□遠端攻擊者可對目標系統之SMBv3服務發送特製請求或架設惡意的SMBv3伺服器誘騙受害者進行連線，導致遠端執行任意程式碼。
- 影響平台:
  - Windows 10 Version 1903 (32與64位元)
  - Windows 10 Version 1909 (32與64位元)
  - Windows Server version 1903
  - Windows Server version 1909
- 建議措施:
  - 目前微軟官方已針對此弱點釋出更新程式，請儘速至下列連結進行更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
- 參考資料:
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv200005
  3. https://thehackernews.com/2020/03/patch-wormable-smb-vulnerability.html
  4. https://thehackernews.com/2020/03/smbv3-wormable-vulnerability.html
  5. https://www.ithome.com.tw/news/136307

計算機與通訊中心
網路系統組 敬啟