行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2020-0031	發布時間	Fri Mar 13 16:50:40 CST 2020
事件類型	漏洞預警	發現時間	Fri Mar 13 00:00:00 CST 2020
警訊名稱	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	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		
影響等級	高		
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		

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw