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-2017-0046	發布時間	Thu Apr 27 12:19:03 CST 2017
事件類型	漏洞預警	發現時間	Tue Apr 25 00:00:00 CST 2017
警訊名稱	微軟伺服器訊息區塊(SMB)協定存在數個安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速進行更新		
內容說明	微軟伺服器訊息區塊(Server Message Block，SMB)又名網路檔案分享系統，是微軟所開發的應用層網路傳輸協定，主要功能是讓網路上的機器能夠共享檔案、印表機、串列埠及通訊等資源。 2017 年 4 月 14 日，國際上名為影子掮客(The Shadow Brokers)的駭客團體，公開釋出新一波的網路攻擊工具，當中多款工具(EternalBlue、EternalRomance、 EternalChampion 及 DoublePulsar 等)鎖定用於 SMB 協定，攻擊者可先透過 EternalBlue 工具發送特製的惡意封包到未進行安全更新且啟用 SMB 協定的作業系統中，並透過 DoublePulsar 工具執行惡意操作指令或下載其他的惡意程式等。導致攻擊者遠端執行任意程式碼。		
影響平台	Windows Vista Windows 7 Windows 8.1 Windows RT 8.1 Windows 10 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016		

影響等級	高
建議措施	微軟官方已針對此弱點釋出修復程式，請儘速至微軟官方網頁(https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx)進行更新。
參考資料	1.http://www.ithome.com.tw/news/113667 2.https://twitter.com/belowzeroday/status/856066791319195648 3.http://thehackernews.com/2017/04/windows-hacking-tools.html

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