張貼日期：2017/05/01

[資安漏洞預警通知] 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

主旨：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。

說明：

1. 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。
2. 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。
3. 影響平臺：
   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
4. 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。
5. 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

---

計算機與通訊中心
網路系統組 敬啟