# 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-2017-0051 | 發布時間 | Sat May 13 12:55:18 CST 2017 |
| 事件類型 | 公告資訊 | 發現時間 | Sat May 13 00:00:00 CST 2017 |
| 警訊名稱 | 近期勒索軟體 WannaCry 活動頻繁，請立即更新作業系統與防毒軟體，並注意平時資料備份作業 | | |
| 內容說明 | 近期加密勒索軟體 WannaCry(WanaCrypt0r 2.0) 的新型變種勒索病毒正利用 Windows 漏洞(MS17-010 漏洞)肆虐，受感染的電腦將會有大量檔案被加密，並且要求高價比特幣贖金。<br><br>此波勒索軟體攻擊是利用微軟伺服器訊息區塊(SMB)協定存在數個安全漏洞，台灣受影響的電腦以 Windows XP/Vista/7/8/8.1 居多，作業系統請立刻進行 Windows Update 檢查並安裝更新。 | | |
| 影響平台 | Windows XP<br><br>Windows Vista<br><br>Windows 7<br><br>Windows 8.1<br><br>Windows RT 8.1<br><br>Windows 10<br><br>Windows Server 2008<br><br>Windows Server 2008 R2<br><br>Windows Server 2012<br><br>Windows Server 2012 R2<br><br>Windows Server 2016 | | |
| 影響等級 | 高 | | |

| | |
|---|---|
| 建議措施 | 1.確實持續更新電腦的作業系統、應用程式及防毒軟體等至最新版本。<br><br>(1)微軟官方已針對此勒索軟體利用之弱點釋出修復程式，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。<br><br>(2)目前微軟 Windows XP 與 Vista 已經不再會有任何更新，如果可以建議將 Windows 升級到最新版作業系統。<br><br>2. 定期備份電腦上的檔案及演練資料還原程序。<br><br>3. 如不幸受到感染，請立即將受害電腦的網路連線及外接儲存裝置拔除，並關閉受害電腦無線網路。建議在清除惡意軟體前不要開啟任何檔案，或變更檔案存放位置。 |
| 參考資料 | 針對微軟伺服器訊息區塊(SMB)協定存在數個安全漏洞相關說明，可參考 106/4/27 發布之 NCCST-ANA-2017-0046 警訊。 |

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