

# 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	Mon May 15 14:22:37 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	[更新]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	<p>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。</p> <p>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。</p>		
影響平台	<p>Windows XP</p> <p>Windows Vista</p> <p>Windows 7</p> <p>Windows 8.1</p> <p>Windows RT 8.1</p> <p>Windows 10</p> <p>Windows Server 2008</p> <p>Windows Server 2008 R2</p> <p>Windows Server 2012</p> <p>Windows Server 2012 R2</p> <p>Windows Server 2016</p>		
影響等級	高		

建議措施	<p>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。</p> <p>(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(<a href="https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx">https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx</a>)進行更新。</p> <p>(2)[更新]針對此次重大威脅，微軟也額外替已超過維護週期之作業系統，例如 XP/8/Server 2003 等釋出修補程式，請參考連結(<a href="https://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598">https://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598</a>)下載後進行更新。</p> <p>2. 定期備份電腦上的檔案及演練資料還原程序。</p> <p>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。</p>
參考資料	<p>1. 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。</p> <p>2. [更新]針對重大漏洞相關說明，可參考技術服務中心官網重大漏洞專區網頁(<a href="https://www.ncst.nat.gov.tw/ImportantSection?lang=zh">https://www.ncst.nat.gov.tw/ImportantSection?lang=zh</a>)。</p>
<p>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 (<a href="https://www.ncert.nat.gov.tw">https://www.ncert.nat.gov.tw</a>) 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。</p> <p>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。</p> <p>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： <a href="mailto:service@ncst.nat.gov.tw">service@ncst.nat.gov.tw</a></p>	