張貼日期:2017/05/29

[資安漏洞預警通知] 近期勒索軟體Petya活動頻繁 , 請立即更新作業系統[Office應用程式與防毒軟體 , 並注意平時資料備份作業

主旨:近期勒索軟體Petya活動頻繁,請立即更新作業系統□Office應用程式與防毒軟體,並注意平時資料備份作業

說明:

1. 全球多個國家於本(106)年6月27日晚間陸續傳出遭勒索軟體Petya攻擊事件,受影響範圍以烏克蘭、俄羅斯及東歐等地區災情最為嚴重□Petya為2016年勒索軟體Petya變種,攻擊者主要利用社交工程郵件誘使使用者開啟附件檔案,藉由攻擊Office RTF漏洞(CVE-2017-0199)執行惡意程式碼,以取得系統控制權,並配合微軟MS17-010漏洞□Windows遠端管理指令Psexec或WMIC(Windows Management Instrumentation Command-line)等方式進行內部擴散,受感染主機之作業系統開機磁區(MBR)與檔案配置表(MFT)將被加密,導致無法進入作業系統,只會在電腦螢幕上看到要求贖金的訊息。

2. 影響平臺:

Windows XP

Windows Vista

Windows 7

Windows 8.1

Windows RT 8.1

Windows 10

Windows Server 2003

Windows Server 2008

Windows Server 2008 R2

Windows Server 2012

Windows Server 2012 R2

Windows Server 2016

3. 建議措施:

- 1. 確實持續更新電腦的作業系統□Office應用程式及防毒軟體等至最新版本□Petya勒索軟體所利用之作業系統弱點與Office應用程式弱點,已分別於3月與4月釋出修復程式,請至微軟官方網頁進行更新或進行Windows Update□
 - (1)MS17-010□https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx。另外已超過維護週期之作業系統,例如XP/Server 2003等,請參考連
 - 結(https://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)下載後進行更新[(2)CVE-2017-0199[https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/C VE-2017-0199
- 2. 更新電腦防毒軟體病毒碼。
- 3. 作業系統登入密碼應符合複雜性原則,並定期變更密碼。
- 4. 定期備份電腦上的檔案及演練資料還原程序。
- 5. 避免開啟來路不明郵件,包含附件與連結。

4. 參考資料

- 1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199
- 2. https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx

計算機與通訊中心

網路系統組 敬啟

From:

https://net.nthu.edu.tw/netsys/ - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/mailing:announcement:20170629_01



