張貼日期：2017/05/12

[資安漏洞預警通知] 微軟惡意程式防護引擎(Microsoft Malware Protection Engine)存在允許攻擊者遠端執行程式碼之漏洞，進而取得系統控制權

主旨：微軟惡意程式防護引擎(Microsoft Malware Protection Engine)存在允許攻擊者遠端執行程式碼之漏洞，進而取得系統控制權，請儘速確認防護引擎版本並進行更新

說明：

1. 微軟自Windows 7版本起內建Windows Defender程式，藉由即時監控、阻擋、隔離或刪除惡意程式功能，保護電腦免於惡意程式危害。本次存在漏洞之惡意程式防護引擎(Microsoft Malware Protection Engine□簡稱MsMpEng)為Windows Defender核心元件，亦是Microsoft Forefront與Microsoft Security Essentials等微軟安全產品的核心元件□MsMpEng中負責掃描與分析的核心元件稱為mpengine□其中NScript是mpengine的元件，用於檢測任何看起來像是JavaScript的文件。Google Project Zero成員Tarvis Ormandy與Natalie Silvano發現MsMpEng 1.1.13701.0(含)以前的版本，如果系統啟用即時保護（預設開啟）功能，攻擊者透過傳送特製檔案□MsMpEng自動掃描該檔案時，因NScript無法正確的解析檔案，導致攻擊者可透過檔案中的JavaScript程式碼利用該漏洞執行任意程式碼，進而獲取系統控制權。
2. 影響平臺：
   Microsoft Forefront Endpoint Protection 2010
   Microsoft Endpoint Protection
   Microsoft Forefront Security for SharePoint Service Pack 3
   Microsoft System Center Endpoint Protection
   Microsoft Security Essentials
   Windows Defender for Windows 7
   Windows Defender for Windows 8.1
   Windows Defender for Windows RT 8.1
   Windows Defender for Windows 10, Windows Server 2016
   Windows Intune Endpoint Protection
3. 建議措施：
   1. 微軟官方已針對此弱點釋出修補程式，其修補方式為更新惡意程式防護引擎為1.1.13704.0版，請參考微軟官方網頁(https://technet.microsoft.com/en-us/library/security/4022344)□
   2. 建議儘速進行檢查與更新，例如Windows 7之Windows Defender惡意程式防護引擎版本之更新方式如下：
      1. 開啟控制台。
      2. 選擇□Windows Defender□□
      3. 於上方工具列，點選最右邊的「說明選項」。
      4. 選擇「關於Windows Defender□□即可看到引擎版本。
      5. 如為1.1.13701.0(含)以前的版本，可從「說明選項」中點選「檢查更新」即可將引擎版本更新至最新版本。
   3. 其他受影響之微軟安全產品檢查與更新方式，請參閱參考資料所述。
4. 參考資料
   1. https://technet.microsoft.com/en-us/library/security/4022344
   2. https://support.microsoft.com/en-us/help/2510781/microsoft-malware-protection-engine-deployment-information

3. http://www.ithome.com.tw/news/114074

計算機與通訊中心
網路系統組 敬啟