張貼日期：2017/05/08

[資安漏洞預警通知] 特定版本Intel晶片韌體中的AMT□SBT及ISM管理技術存在安全漏洞，允許攻擊者遠端獲取系統的控制權限

主旨：特定版本Intel晶片韌體中的AMT□SBT及ISM管理技術存在安全漏洞，允許攻擊者遠端獲取系統的控制權限

說明：

1. 英特爾(Intel)主動管理技術(Active Management Technology□AMT)是內嵌於英特爾vPro 架構平台的一項管理功能，獨立於作業系統外運行，即使主機已經關閉，只要主機仍與電源線和網絡相連，遠端管理人員仍可以存取Intel AMT□而服務管理器(Intel Standard Manageability□ISM)則具有遠端關機、開機、重新開機及監視運行的應用程式等，至於小型企業技術(Small Business Technology□SBT)□則具有本機端的軟體監控器、資料備份和復原及省電功能等。
2. 研究人員Maksim Malyutin發現特定Intel晶片韌體中的AMT□SBT及ISM管理技術存在安全漏洞(CVE-2017-5689)□目前已知攻擊者可在未授權的情況下透過AMT管理技術遠端或本地端獲取系統控制權限，像是開機、關機、讀取文件、檢查正執行的程序、追蹤鍵盤/滑鼠及螢幕畫面等。
3. 影響平臺□ First-gen Core family:
4. 建議措施：
    1. 目前Intel官方已針對此弱點釋出修復韌體，請參考Intel官方網頁(https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr)，或洽詢合作之OEM廠商更新至相對應的韌體版本，詳細修復韌體版本如下：
        1. First-gen Core family: >= 6.2.61.3535的版本。
        2. Second-gen Core family: >= 7.1.91.3272的版本。
        3. Third-gen Core family: >= 8.1.71.3608的版本。
        4. Fourth-gen Core family: >= 9.1.41.3024的版本。
        5. Fourth-gen Core family: >= 9.5.61.3012的版本。
        6. Fifth-gen Core family: >= 10.0.55.3000的版本。
        7. Sixth-gen Core family: >= 11.0.25.3001的版本。
        8. Seventh-gen Core family: >= 11.6.27.3264的版本。
    2. Intel官方網頁(https://downloadmirror.intel.com/26755/eng/INTEL-SA-00075%20Detection%20Guide-Rev%201.0.pdf)釋出之檢測韌體版本方法，詳細檢測步驟如下：
        1. 下載Intel® SCS System Discovery Utility工具(https://downloadcenter.intel.com/download/26691/Intel-SCS-System-DiscoveryUtility)□
        2. 以系統管理員啟動cmd視窗。
        3. 鍵入SCSDiscovery.exe SystemDiscovery /noregistry產生一份XML檔，並檢視該份文件中的FWVersion值，確認是否為上述受影響之韌體版本。
    3. Intel官方網頁(https://downloadmirror.intel.com/26754/eng/INTEL-SA-00075%20Mitigation%20Guide-Rev%201.1.pdf)釋出之關閉AMT□ISM及SBT方法，詳細關閉步驟如下：
        1. 以系統管理員權限啟動cmd視窗。
        2. 鍵入sc config LMS start= disabled(注意disabled前有一空格)。
5. 參考資料
    1. http://www.ithome.com.tw/news/113815

2. https://www.bleepingcomputer.com/news/hardware/intel-fixes-9-year-old-cpu-flaw-that-allows-remote-code-execution/
3. https://www.theregister.co.uk/2017/05/01/intel_amt_me_vulnerability/

計算機與通訊中心

網路系統組 敬啟