張貼日期：2017/11/28

[資安漏洞預警通知]特定Intel處理器中的ME、SPS及TXE管理技術存在多個安全漏洞，允許攻擊者遠端執行任意程式碼，或本地端進行提權與執行任意程式碼

主旨：特定Intel處理器中的ME、SPS及TXE管理技術存在多個安全漏洞，允許攻擊者遠端執行任意程式碼，或本地端進行提權與執行任意程式碼

說明：

1. 研究人員發現Intel管理引擎(Management Engine、ME)、受信任的執行引擎(Trusted Execution Engine、TXE)及伺服器平台服務(Server Platform Services、SPS)存在多個安全漏洞。
2. 當中管理引擎(ME)包含CVE-2017-5705、CVE-2017-5708、CVE-2017-5711及CVE-2017-5712安全漏洞，受信任的執行引擎(TXE)包含CVE-2017-5707與CVE-2017-5710安全漏洞，伺服器平台服務(SPS)包含CVE-2017-5706與CVE-2017-5709安全漏洞。其中部分漏洞允許攻擊者於本地用戶的目標系統進行提權與執行任意程式碼。
3. 影響平臺：
    1. 處理器版本：
       6th, 7th, and 8th generation Intel Core Processor Family
       Intel Xeon Processor E3-1200 v5 and v6 Product Family
       Intel Xeon Processor Scalable Family
       Intel Xeon Processor W Family
       Intel Atom C3000 Processor Family
       Apollo Lake Intel Atom Processor E3900 series
       Apollo Lake Intel Pentium Processors
       Intel Celeron N and J series Processors
    2. 韌體版本：
       Intel Manageability Engine韌體版本、8.x、9.x、10.x、11.0.x.x
       11.5.x.x、11.6.x.x、11.7.x.x、11.10.x.x、11.20.x.x
       Intel Server Platform Services韌體版本、4.0.x.x
       Intel Trusted Execution Engine韌體版本、3.0.x.x
4. 建議措施：
    1. 目前Intel官方已針對該弱點成立專區(https://www.intel.com/content/www/us/en/support/articles/000025619/software.html)，並彙整各家受影響廠商的技術支援連結，請持續關注或洽詢合作之OEM廠商更新至相對應的韌體版本，詳細修復韌體版本如下：
        - 6th Generation Intel Core Processor Family大於Intel ME 11.8.50.3425的版本
        - 6th Gen X-Series Intel Core Processor大於Intel ME 11.11.50.1422的版本
        - 7th Generation Intel Core Processor Family大於Intel ME 11.8.50.3425的版本
        - 7th Gen X-Series Intel Core Processor大於Intel ME 11.11.50.1422的版本
        - 8th Generation Intel Core Processor Family大於Intel ME 11.8.50.3425的版本
        - Intel Xeon Processor E3-1200 v5 Product Family大於Intel ME 118.50.3425與Intel SPS 4.1.4.054的版本
        - Intel Xeon Processor E3-1200 v6 Product Family大於Intel ME 118.50.3425與Intel SPS 4.1.4.054的版本

- Intel Xeon Processor Scalable Family大於Intel ME 11.21.50.1424與Intel SPS 4.0.04.288的版本
- Intel Xeon Processor W Family大於Intel ME 11.11.50.1422的版本
- Intel Atom C3000 Processor Family大於Intel SPS 4.0.04.139的版本
- Apollo Lake Intel Atom Processor E3900 series大於Intel TXE Firmware 3.1.50.2222的版本
- Apollo Lake Intel Pentium大於Intel TXE Firmware 3.1.50.2222的版本
- Celeron N series Processors大於Intel TXE Firmware 3.1.50.2222的版本
- Celeron J series Processors大於Intel TXE Firmware 3.1.50.2222的版本

2. Intel官方網頁釋出之檢測工具，詳細檢測步驟如下：
    1. 下載Intel SCS System Discovery Utility工具(https://downloadcenter.intel.com/download/27150)
    2. Windows執行Intel-SA-00086-GUI.exe程式
    3. Linux執行intel_sa00086.py程式

5. 參考資料:
    1. https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr
    2. https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr

---

計算機與通訊中心
網路系統組 敬啟