張貼日期：2017/11/27

［資安漏洞預警通知］英飛凌TPM晶片存在RSA缺陷漏洞(CVE-2017-15361)導致攻擊者可偽冒合法使用者以獲取機敏資訊，請儘速評估確認與進行修正

主旨：英飛凌TPM晶片存在RSA缺陷漏洞(CVE-2017-15361)導致攻擊者可偽冒合法使用者以獲取機敏資訊，請儘速評估確認與進行修正

說明：

1. 英飛凌(Infineon Technologies)是一間位於德國的半導體製造商，主力提供半導體與系統解決方案。可信賴平台模組(Trusted Platform Module, TPM)是由可信賴運算組織(Trusted Computing Group, TCG)所發展的安全晶片規格，用以儲存如密碼、憑證或加密金鑰等重要資料，目前廣泛應用於筆記型電腦、路由器或物聯網裝置的主機板上。
2. 研究人員發現英飛凌公司的加密智能卡、安全令牌(Security Tokens)及其他安全硬體等，其基於TCG規範1.2與2.0版所生產的TPM晶片存在RSA缺陷漏洞(CVE-2017-15361)攻擊者可透過因數分解攻擊(Factorization Attack)計算出私密金鑰(Private Key)進而導致攻擊者可偽冒合法使用者以獲取機敏資訊。
3. 影響平臺：　基於TCG規範1.2與2.0版所生產之TPM晶片
4. 建議措施：
    1. 目前英飛凌官網(https://www.infineon.com/cms/en/product/promopages/tpm-update/?redirId=59160)已彙整各廠商所提供技術支援連結，各機關可自行參考廠商提供的受影響產品與更新檔進行修復。
        - HP (https://support.hp.com/us-en/document/c05792935)
        - Lenovo (https://support.lenovo.com/tw/zh/product_security/len-15552)
        - Fujitsu (http://support.ts.fujitsu.com/content/InfineonTPM.asp)
        - Panasonic (http://pc-dl.panasonic.co.jp/itn/info/osinfo20171026.html)
        - Toshiba (https://support.toshiba.com/sscontent?contentId=4015874)
        - Chrome OS (https://sites.google.com/a/chromium.org/dev/chromium-os/tpm_firmware_update)
5. 參考資料:
    1. https://crocs.fi.muni.cz/public/papers/rsa_ccs17#detection_tools_mitigation_and_workarounds
    2. https://www.ithome.com.tw/news/117518
    3. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170012
    4. http://www.securityweek.com/tech-giants-warn-crypto-flaw-infineon-chips

---

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:20171127_01

Last update: **2017/11/28 10:39**