行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2017-0048	發布時間	Wed May 03 09:55:45 CST 2017
事件類型	漏洞預警	發現時間	Tue May 02 00:00:00 CST 2017
警訊名稱	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(CVE-2017-5689)，允許攻擊者遠端獲取系統的控制權限		
內容說明	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。 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。		
影響平台	First-gen Core family: < 6.2.61.3535 個系列版本 Second-gen Core family: < 7.1.91.3272 個系列版本 Third-gen Core family: < 8.1.71.3608 個系列版本 Fourth-gen Core family: < 9.1.41.3024 個系列版本 Fourth-gen Core family: < 9.5.61.3012 個系列版本 Fifth-gen Core family: < 10.0.55.3000 個系列版本 Sixth-gen Core family: < 11.0.25.3001 個系列版本 Seventh-gen Core family: < 11.6.27.3264 個系列版本		
影響等級	高		

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)

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/

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw