

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2014081208080808	發佈時間	2014-08-12 09:06:23
事故類型	ANA-漏洞預警	發現時間	2014-08-06 00:00:00
影響等級	中		

[主旨說明:]請各機關確認所屬系統平台(含個人電腦、工作站主機及伺服器)是否支援 Intel 主動管理技術(Active Management Technology, AMT)，並設定停用或條件式開放該項功能

[內容說明:]

轉發國家資通安全會報 技術服務中心 漏洞/資安訊息警訊 ICST-ANA-2014-0016

近期接獲通報，Intel 晶片的主動管理技術可在未經授權下，喚醒已關機的電腦，並利用該技術的 KVM 功能(使用鍵盤、螢幕及滑鼠)，竊取該平台之敏感資訊。

Intel 公司於 2010 年將遠端 KVM 管理功能加入主動管理技術中，並利用網路通訊埠 16992、16993、16994 及 16995 進行連線與管理，且該技術於部分平台預設為啟用狀態。

為確保平台安全性，請各機關確認所屬系統主機板是否支援 Intel 主動管理技術(AMT)並設定關閉，以防止遭受相關攻擊。

[註]請各機關自行確認系統主機板使用與設定情況即可，無須另行回報。

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發

[影響平台:]

配載 Intel vPro 晶片之系統平台(個人電腦、工作站主機與伺服器)

(搭載 Intel vPro 技術之 Intel Core 處理器的電腦系統，以及 Intel Xeon3400 系列處理器的工作站平台)

[建議措施:]

1. 檢視該主機板是否支援 vPro 功能或黏貼之貼紙含有 vPro 或 XEON (Xeon 3400 系列)字樣。

2. 將 AMT 功能列為管制項目，定期檢查 AMT 功能有無啟用，並以原則關閉例外開放之方式進行管理，即預設停用 AMT 功能，如有使用需求，應由管理員管理密碼，除定期修改預設密碼外，密碼並應具備複雜度強度。

3. 因各家主機板 BIOS 格式不同，技服中心僅提供常見 BIOS 作為範例。停用 AMT 功能：於開機時點擊 DEL 或 F2 進入 BIOS→按 F7 進入進階模式→將分頁移至 Advanced→於 AMT 項目按 Enter→將 Enable 改為 Disable→按 F10 點選 YES 存檔離開。
4. 防火牆應針對 AMT 所使用的通訊埠進行監控管制，若非申請使用之需求，應停用通訊埠為 16992、16993、16994 及 16995 之流量；申請使用之需求也應在防火牆設定點對點存取，避免未經授權的來源進行存取。
5. 為避免機敏資訊經由網路傳輸，處理機敏公務之設備，應採實體隔離作業。

[參考資料:]

參考資料

- 1.<http://www.intel.com/content/www/us/en/architecture-and-technology/intel-active-management-technology.html>
- 2.<http://support.radmin.com/index.php?/Knowledgebase/Article/View/9/9/how-to-set-up-intel-amt-features>
- 3.http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100402-Vassilios_Ververis-with-cover.pdf
- 4.<http://www.ihome.com.tw/node/43886>
- 5.ftp://ftp.dell.com/Manuals/all-products/esuprt_laptop/esuprt_precision_mobile/precision-m4500
- 6.<http://www.intel.com.tw/content/www/tw/zh/architecture-and-technology/intel-active-management-technology.html>
- 7.<http://www.intel.com.tw/content/dam/www/public/us/en/documents/best-practices/using-intel-vpro-technology-with-a-centralized-it-support-portal-paper.pdf>

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。國家資通安全會報 技術服務中心
(<http://www.icst.org.tw/>)

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@icst.org.tw