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	ICST-ANA-2014-0016	發布時間	Fri Aug 08 15:36:35 CST 2014
事件類型	漏洞預警	發現時間	Wed Aug 06 00:00:00 CST 2014
警訊名稱	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	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。		
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)		
影響等級	中		
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(詳見附件圖檔)。 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。