因應微軟Windows 7作業系統終止支援服務之防護措施建議

行政院國家資通安全會報技術服務中心

108年12月

大綱

- 前言
- Windows 7終止支援對資安影響
- 防護措施建議
- Windows 7終止支援服務專區
- 結語

前言

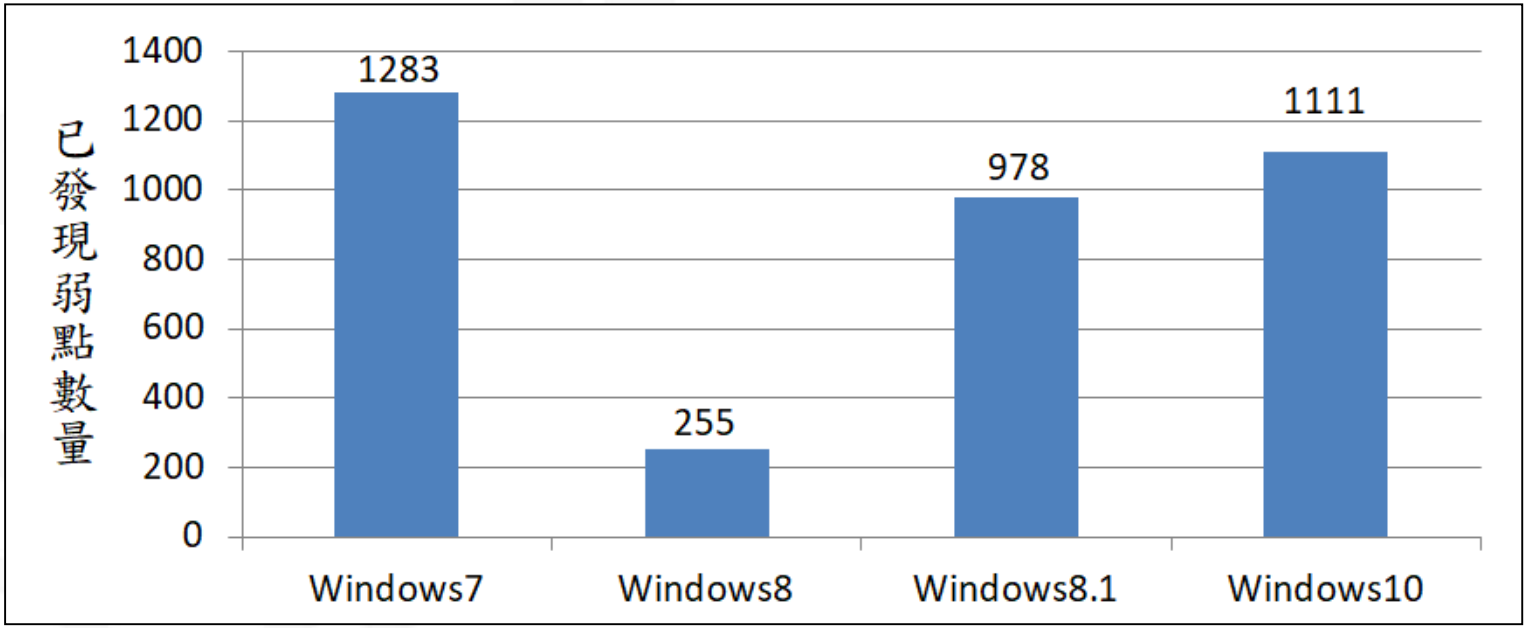
- 微軟2009年推出Windows 7，雖然歷經Windows 8、Windows 8.1到現在的Windows 10，至今已經過10年，仍有近30%市占率
- 自2017/10/31起停售Windows 7後，隨著時間的演進，已進入產品生命週期末端，將於2020/1/14終止支援(End of Support，簡稱EOS)，不再針對Windows 7提供下述支援服務：
  - 安全性更新
  - 非安全性修補程式及功能更新
  - 產品技術支援及線上技術內容更新
- 仍使用Windows 7主機之機關，請參考本建議進行更新或防護評估，以避免成為資安風險

Windows 7終止支援對資安影響(1/3)

- Windows 7作業系統相關應用軟體弱點已無法確保可取得更新的修補程式
  - Windows 7作業系統上所安裝之Internet Explorer 11瀏覽器於2020/1/14後也將無法取得新的修補程式
  - 微軟應用程式開發與執行環境(Runtime)的支援平台也會調整(如.NET Framework與Visual C++可轉散發套件)，相對應在Windows 7上的安全性更新也不再支援
  - Windows 7終止支援後，將面臨應用程式無法開發維護、系統效能、重大資安風險等挑戰

Windows 7終止支援對資安影響(2/3)

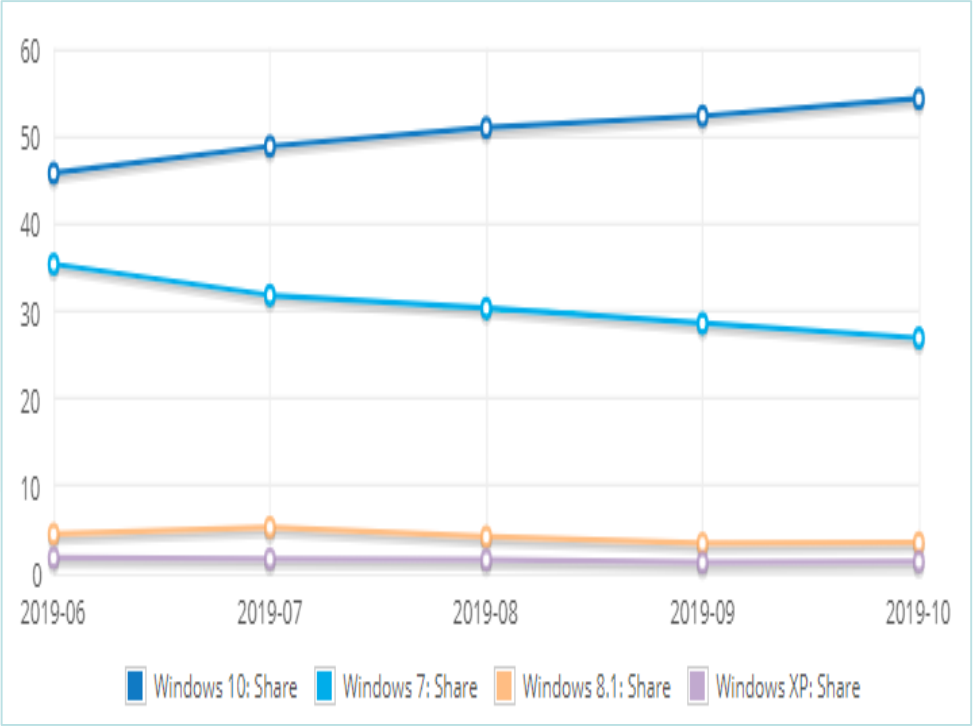
- Windows 7作業系統已發現弱點數量多，遭攻擊風險高
  - 根據CVE Details弱點資料庫統計數據顯示， Windows 7作業系統已被發現弱點數量達1,283個，高於Windows 8.1與Windows 10



Windows 7終止支援對資安影響(3/3)

- 微軟基於下列原因建議升級至Windows 10
  - 提供高度安全的內建保護，協助抵禦現代安全威脅
  - 可與現有基礎架構整合，繼續使用現有應用程式

- 據 NetApplications 研究
  - Windows 7市占率已降低至30%以下
  - Windows 10市占率提高至50%以上
  - 代表市場上已逐步轉移至Windows 10



防護措施建議

事件通報

政府機關

1. 加速Windows 7升級至Windows新版作業系統
2. 強化Windows 7電腦資安防護
3. 透過網路區隔加強管理使用Windows 7電腦

技服中心

4. 執行Windows 7弱點持續監測計畫

資安資訊分享

1.加速Windows 7升級至新版作業系統

- Windows 7升級至Windows新版作業系統為根本解決之道
- Windows 10已於2015/7/29上市，請各機關加速Windows 7升級作業
- 若機關發現資安事件入侵原因來自Windows 7弱點，則可能該機關已遭鎖定，屬「Windows 7高風險機關」，應先進行Windows 7升級作業

2.強化Windows 7電腦資安防護

- 微軟公司終止支援後，仍需持續使用Windows 7電腦之機關應規劃與部署資安防護強化措施，建議由以下4方面進行：
  - 部署Windows 7 GCB
  - 帳戶權限設定
  - 軟體防護
  - 監控防禦

2.1部署Windows 7 GCB

- 部署Windows 7 GCB，藉由規範電腦之組態安全設定(如：密碼長度、更新期限等)，強化資安防護

技服中心GCB專區：https://www.nccst.nat.gov.tw/GCB

2.2帳戶權限設定

- 賦予使用者帳戶符合業務需求之最小權限，儘量避免使用管理者權限登入系統，以降低攻擊者取得電腦完整主控權之機會
- 建立新的管理員帳號進行系統管理，並停用本機預設管理者帳號「Administrator」，以避免攻擊者直接鎖定「Administrator」帳號進行攻擊

2.3軟體防護(1/2)

- 若無使用需求，請停止使用IE瀏覽器，改採其他如Google Chrome或Mozilla Firefox等仍會提供更新服務之替代瀏覽器，以提升瀏覽網頁之安全
- 建立允許使用者執行的已授權軟體完整清單，並利用Windows 7內建之「軟體限制原則(Software Restriction Policies)」功能，確保只有已授權軟體能在電腦上執行

2.3軟體防護(2/2)

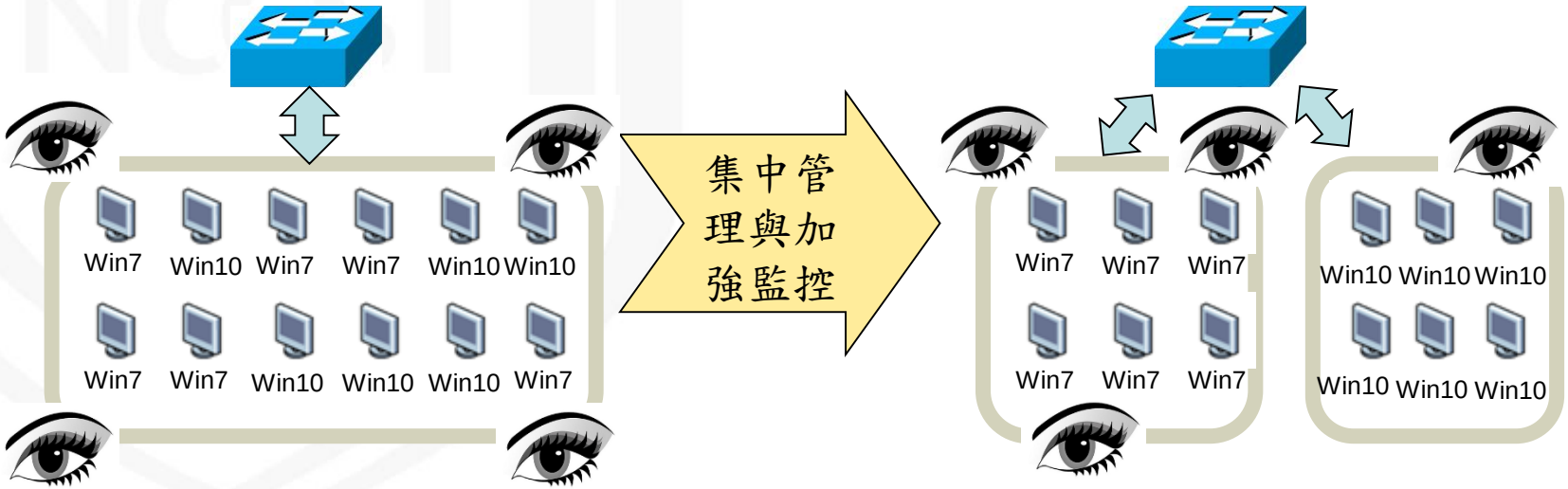
- 針對已安裝之所有應用程式即時進行更新，避免應用程式漏洞危害系統安全

2.4監控防禦

- 確實安裝防毒軟體，即時更新病毒碼，並至少每週執行一次完整掃描與檢視防毒軟體掃描紀錄
- 安裝主機端入侵防禦系統(H-IPS)，提升Windows 7電腦防禦能力
- 在閘道端部署防火牆設備，並透過嚴謹的白名單管理機制，有效管理網路連線行為
- 利用安全資訊與事件管理(SIEM)進行跨設備關聯式分析與監控，確實掌握使用Windows 7電腦之資安事件與安全防護狀態

3.透過網路區隔加強管理Windows 7電腦

- 機關內若同時存在不同作業系統版本之電腦，可利用虛擬區域網路(VLAN)進行網路區隔，將Windows 7電腦放入獨立VLAN，除便於進行集中管理外，亦可避免影響其他VLAN內之電腦
- 針對風險較高之Windows 7電腦VLAN可加強網路流量監控，以有效掌握異常連線行為



4.執行Windows 7弱點持續監測計畫

- 蒐集共通弱點與揭露(CVE)網站、美國國家弱點資料庫(NVD)、微軟公司網站及其他相關安全性網站Windows 7弱點資訊
- 針對新發現之Windows 7弱點資訊，由技服中心即時通知各機關注意
- 定期彙整政府機關已通報之Windows 7相關資安事件，掌握整體影響情形
- 建置「Windows 7終止支援服務專區」，提供「檔案下載」與「FAQ」服務

Windows 7終止支援服務專區

- 檔案下載：提供「因應微軟Windows 7作業系統終止支援服務之防護措施建議」說明文件、操作影片、Windows 7 GCB GPO檔及LocalGPO使用說明等資訊
- FAQ：提供相關常見問題說明
- 網址：https://www.nccst.nat.gov.tw/Win7EndOfSupportIntro

結語

- 微軟公司已確定2020/1/14終止Windows 7支援服務，各機關應盡速了解機關內部Windows 7使用情形，掌握可能產生之影響，並針對處理重要業務之電腦，優先完成升級
- 對於無法更新Windows 7之電腦，應儘速透過Windows 7之安全性設定與帳戶權限管控等措施，強化主機系統的安全。同時規劃與部署資安防護強化措施，透過網路區隔加強使用Windows 7電腦管理，針對風險較高之使用Windows 7電腦VLAN，加強網路流量監控
- 技服中心將持續進行Windows 7弱點監測與通報作業，蒐集Windows 7弱點資訊，並彙整政府機關通報之Windows 7相關資安事件，以掌握Windows 7資安事件與影響程度

報告完畢
敬請指教