臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

Windows XP 終止支援後之防護策略

臺灣大學計資中心網路組
北區學術資訊安全維運中心

摘要

Windows XP 於 2014 年 4 月 8 日終止支援，而仍有許多企業機構、學校單位因為慣用程式、開發環境或相容性等等因素仍持續使用 Windows XP 系統。

截至 2014 年 9 月，在 CVE 弱點資料庫中，Windows XP 為 Microsoft 系列產品中已知弱點總數最高的產品，數量高達 728 筆，約為 Windows 7 的兩倍之多，而且數量仍持續成長中。漏洞並不會因為終止支援而不再出現，Windows XP 缺乏修補程式的支援，面臨的風險只會水漲船高。

還好我們仍有一些方式能夠提升 Windows XP 的使用安全性，並降低在這段過渡時期的風險，但最佳的處理方式仍然是更換作業系統。

為了因應各單位的不同需求與建置成本，此份報告將會說明數個能夠著手進行的方向，提供給各單位參考。

基本防禦措施

無論在何種環境，我們都需對 Windows XP 建立必要的基本防禦措施。

1. **安裝防毒軟體**
2. **停用不需要的服務**
3. **停用不使用的 tcp/udp port**
4. **使用更安全的瀏覽器**
5. **建立可靠的還原機制**
6. **利用登錄檔取得更新**

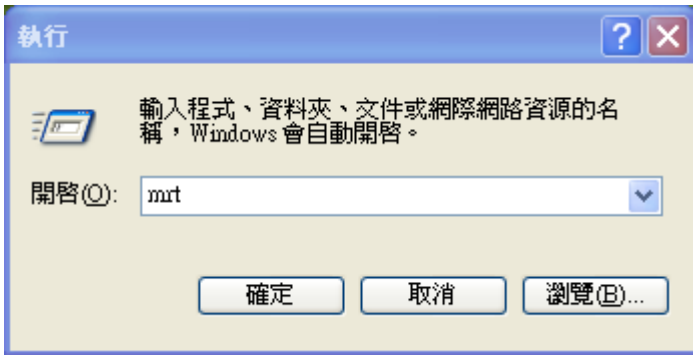
安裝防毒軟體

防毒軟體仍是主動或被動檢測惡意程式的基本防線，即使在作業系統停止支援後，仍能繼續保持一定程度的系統安全。

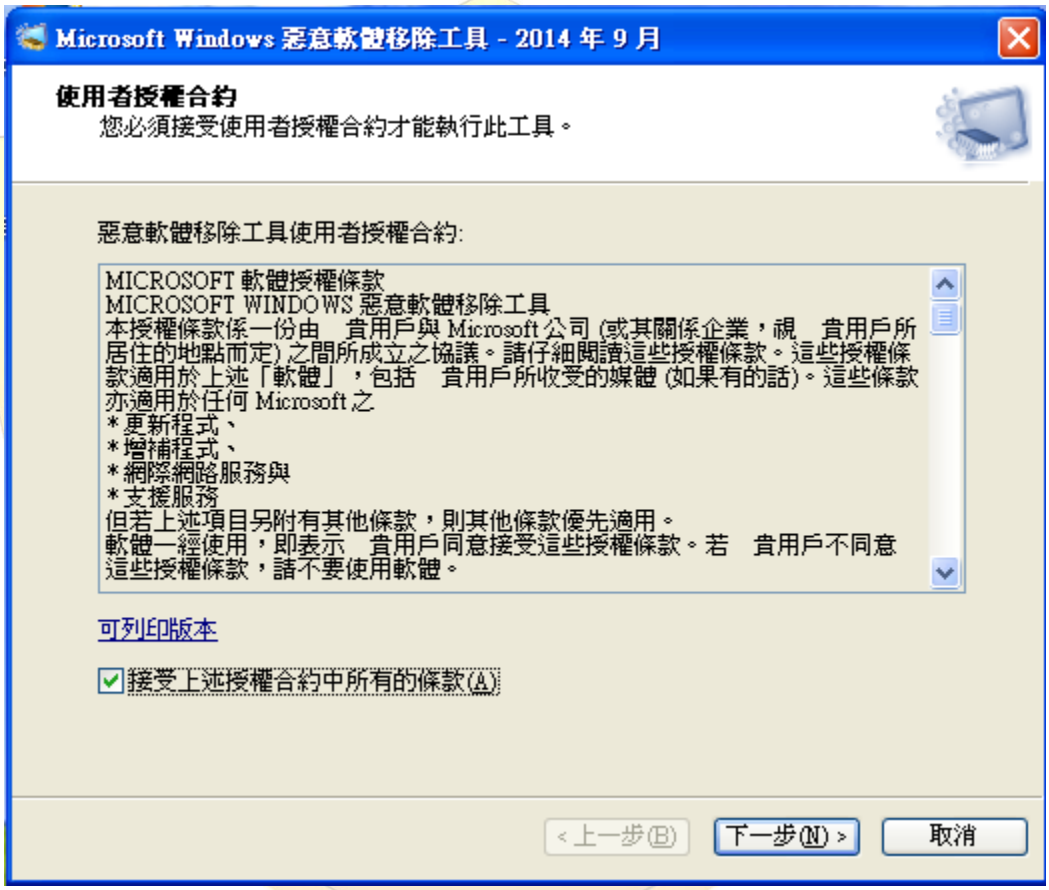
除了防毒軟體以外，微軟公司也提供移除工具，能將主機中常見的惡意軟體移除。此軟體內建於 Windows 作業系統中，並會隨 Windows update 更新。建議可以定期使用此工具，保護電腦不受惡意軟體侵害。

此工具的開啟方式如下：

在執行打入 mrt 並按下確定，即可開啟惡意軟體移除工具。

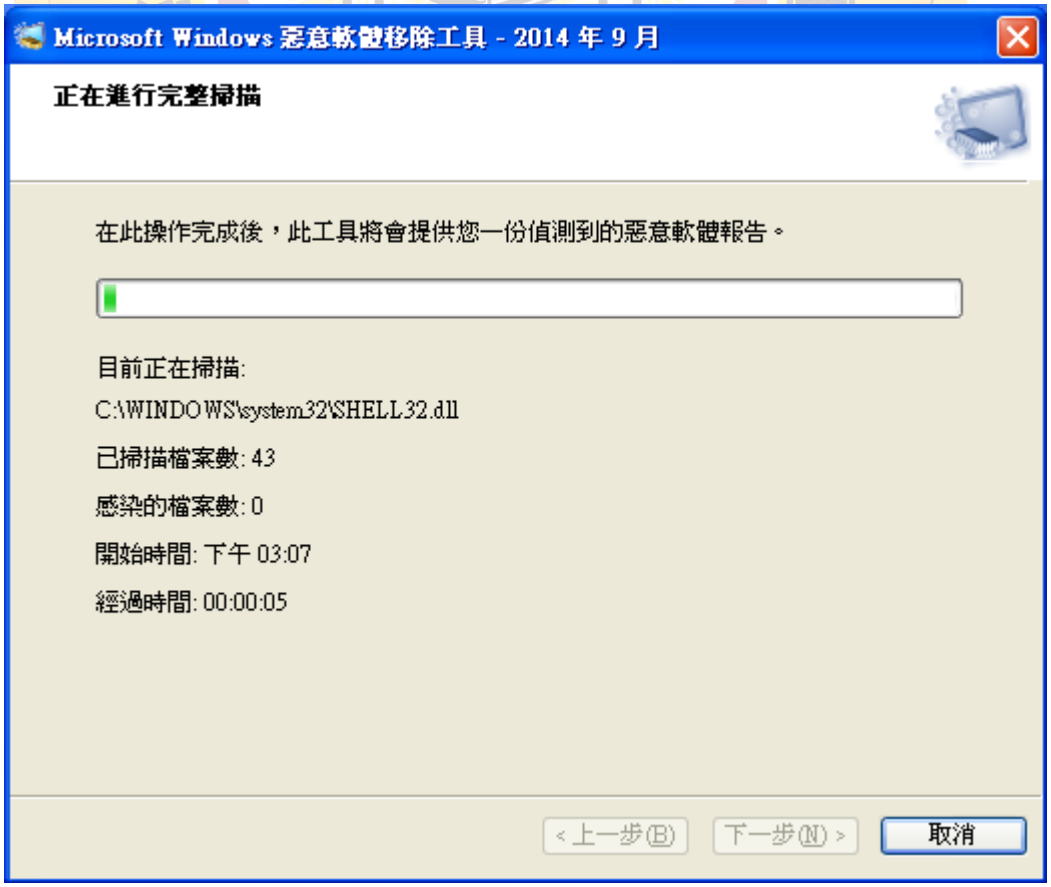


勾選接受上述合約中所有的條款欄位後，按下確定。



按下一步開始掃描。


Microsoft Windows 惡意軟體移除工具 - 2014 年 9 月
歡迎使用 Microsoft Windows Malicious Software Removal Tool
此工具會掃描及自動移除普及的惡意軟體
若要取得此工具的詳細資訊，請瀏覽線上文件。
檢視此工具偵測到並已移除的惡意軟體清單。
此工具並不能取代防毒產品。若要協助保護您的電腦，您應該使用防毒產品。若要取得詳細資訊，請瀏覽 保護您的電腦。
< 上一步(B)
下一步(N) >
取消


Microsoft Windows 惡意軟體移除工具 - 2014 年 9 月
正在進行完整掃描
在此操作完成後，此工具將會提供您一份偵測到的惡意軟體報告。
目前正在掃描:
C:\WINDOWS\system32\SHELL32.dll
已掃描檔案數: 43
感染的檔案數: 0
開始時間: 下午 03:07
經過時間: 00:00:05
< 上一步(B)
下一步(N) >
取消

在掃描完畢後，此工具可協助移除電腦中的惡意程式。

若在執行內輸入 mrt 卻無法找到應用程式時，可以到下列網站下載：

http://www.microsoft.com/zh-tw/download/malicious-software-removal-tool-details.aspx

停用不使用的 tcp/udp port

停用不需使用的通訊埠(port)能夠降低被攻擊與被入侵的風險。

使用更安全的瀏覽器

截至 2014 年 9 月，在 CVE 弱點資料庫中，Internet Explorer 為僅次於 Windows XP 高漏洞數量的產品之一，其漏洞數量為 631 筆。盡可能使用其他安全的瀏覽器作為主要使用的瀏覽器。

Mozilla Firefox https://mozilla.com.tw/firefox/download/

Google Chrome https://www.google.com/intl/zh-TW/chrome/

建立可靠的還原機制

不使用內建的還原系統，而是利用 ghost 或第三方工具對重要磁碟區製作完整映像檔，以作為未來還原之用。

利用登錄檔取得更新

雖然 Windows XP 於 2014 年 4 月 8 日終止支援，但我們可以利用不同作業系統的更新取得安全性修補工具。

Windows Embedded POSReady 是基於 Windows XP SP3 環境之上所設計的作業系統，微軟對於該系統的更新支援到 2019 年 4 月，而微軟針對該作業系統所提供的修補工具在一定程度上對 Windows XP 系統也能夠具有防護的效果，但畢竟不是針對 Windows XP 系統所提供之修補工具，有可能無效或對影響系統正常運作，若要使用此方案時請務必審慎考量。

要達成這樣的目的，我們只需要建立一個簡單的登錄檔，就可以讓 Windows Update 網站將目前所使用的 XP 系統被識別為 Windows Embedded POSReady。

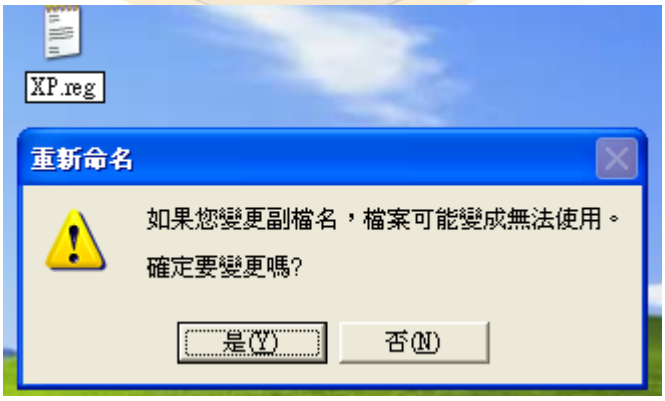
以下步驟為 Windows XP 系統登錄檔的新增方式：

1. 建立一個純文字文件 (副檔名為 txt 型態)

2. 文件內貼上下列內容

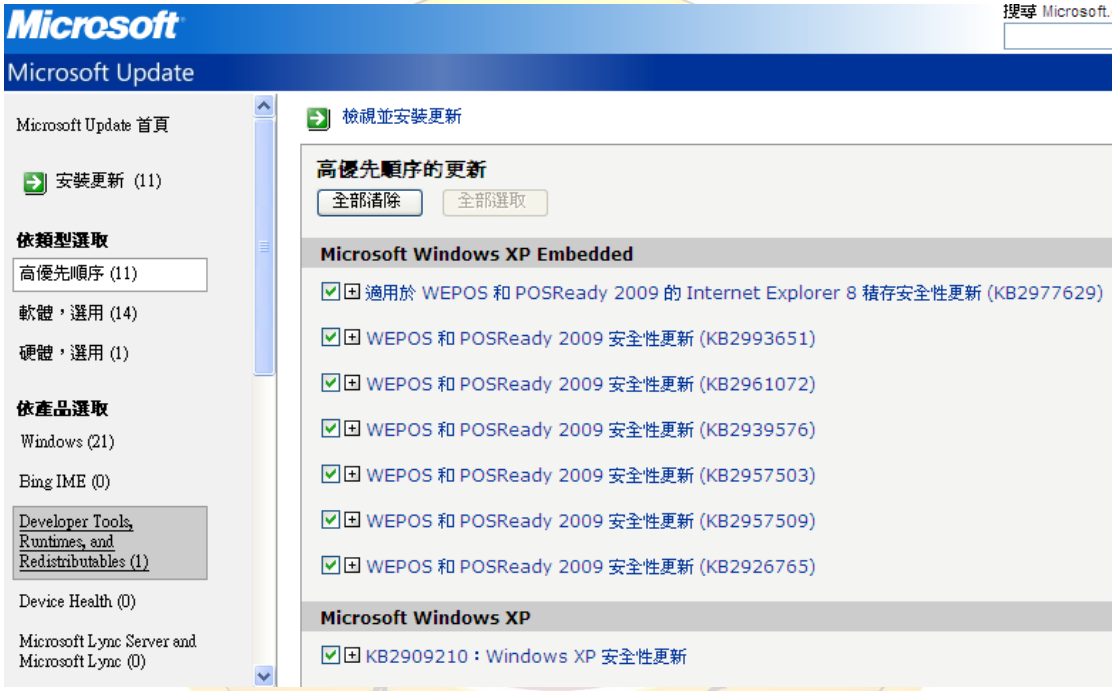
```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\WPA\PosReady]
"Installed"=dword:00000001
```

3. 儲存文件，並更名為 XP.reg (請注意要將副檔名從 txt 改為 reg)



4. 執行 XP.reg

5. 開啟 Windows Update 網站並尋找更新



當 Windows Update 內能夠看到 Microsoft Windows XP Embedded 項目更新，就成功完成了這一次的登錄檔新增，並能為 Windows XP 持續帶來安全性防護直到 2019 年 4 月。

另外此方法只針對 32 位元系統有效，而 64 位元系統需逐一下載 Windows Server 2003 64 位元系統的更新檔，並利用替換更新檔內的 update.ini(不一定每個更新檔都具備此檔案)才能正常安裝到 64 位元系統上。

以下連結為針對 64 位元系統更新的詳盡說明

https://sebijk.com/community/board9-community/board5-pc/2985-getting-xp-updates/?s=78aee0506c40aedfb524ce20bec1ddc9fc1f4010

進階防禦措施

現今大部分的單位逐步進行作業系統更新，而部分主機可能因為連接設備所需、資料庫、無法變更作業系統的應用程式等等因素，仍維持在 Windows XP 環境進行使用。與基本防禦相較，進階防禦措施能夠進一步降低使用 Windows XP 的風險。

1. **外部網路隔離**
2. **雲端操作**
3. **入侵防護**
4. **虛擬化**

進階防禦措施說明如下。

外部網路隔離

外部網路隔離是將使用 Windows XP 之設備以不直接接觸外部網路為主軸的做法。依照各使用環境的不同，將使用 Windows XP 設備放在無連接外部網路的內部網路。

若需要執行一般的網路服務，請盡可能在其他安全的作業系統中執行；但若是 Windows XP 設備必須與外部網路取得資料才能執行必要的服務時，除了確實建立基本防禦措施，建議設置代理伺服器，並透過代理伺服器傳輸資料以確保 Windows XP 設備不會連接外網，或是參考「入侵防護」的防禦措施。

雲端操作

由於 Windows XP 被入侵的風險較高，單位的機敏資料若存放於 Windows XP 設備上，其安全性非常令人擔憂，這部分建議使用可信任的雲端服務提供商為存放資料的平台，並能夠將安全風險轉嫁於雲端服務提供商。對於重視機敏資料安全的單位而言，此作法與自行建置系統及佈署防禦機制比較的話，能夠以低成本並獲取一定程度安全性的策略。

若是單位內想建置自己的雲端伺服器平台，有高成本及安全性的問題需考量，安全性的部分可以再參考「入侵防護」的防禦措施。

入侵防護

入侵防護是除了既有的防火牆設備之外，再利用入侵偵測防護系統(IPS)保護單位所有設備，雖然可提高防禦惡意入侵，但需要投入很高的成本建置及維護。

除了單位在環境中佈署 IPS 外，也可以請 ISP 電信業者或資安公司提供入侵偵測防禦服務，以獲取優質的防禦能力。

虛擬化

虛擬化是將目前無法轉移作業系統的設備轉為以虛擬環境的方式運作，可利用工具達成，如 VMware vCenter Converter，進行 P2V(Physical to Virtual)，並放入虛擬環境執行並持續提供原有的服務。

虛擬化能將數個實體設備上的系統運作轉移到單一設備上，能夠大幅度簡化管理工作。此外，在虛擬化環境中，我們能夠便利且快速地進行備份及災害後的復原工作。我們可以將仍需 Windows XP 環境的平台與系統進行虛擬化，並建置或轉移在具有安全作業系統的設備上，此種方式除了具備安全性以外，還可提高其管理性，有效減少管理者對 Windows XP 設備系統的管理時間。

參考資料

https://sebijk.com/community/board9-community/board5-pc/2985-getting-xp-updates/?s=78aee0506c40aedfb524ce20bec1ddc9fc1f4010