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

重要資訊服務作業系統注意事項:

Windows Server 2003 終止支援後升級與資安防護之道

臺灣大學計資中心網路組

北區學術資訊安全維運中心

目錄

265. 180 WU . ## 300	
目錄	. 2
摘 <mark>要</mark>	. 3
W <mark>indows Server 2003</mark> 如何升級	. 3
如何查看主機 Windows Server 版本與 Patch 更新	. 4
Windows Server 2003 升級前的防禦措施	. 7
參考 <mark>資料</mark>	11

摘要

Windows Server 2003 即將於2015 年7月14日終止支援(End of Support, EOS)。 依據以往經驗,伺服器升級評估與移轉需要費時至少六個月至一年不等,如不盡 快升級作業系統,屆時使伺服器管理者將面臨下列三個問題:

- 1. 資訊安全的風險增高
- 2. 管理成本提高。
- 3. 法規(ISO27001)風險及通過認證難度增加。

本報告說明使用 Windows Server 2003 為重要資訊服務之作業系統時,當 Windows Server 2003 終止支援因應之道及升級策略,以確保應有之資安防護。

Windows Server 2003 如何升級

微軟官方提供 Windows Server 2003 升級建議步驟,依序為:

1. 資產確認與盤點:

想確認組織內部 Windows Server 2003 的伺服器數量,微軟提供工具協助 盤點軟硬體資產, MAP (Microsoft Assessment and Planning Toolkit),可由組 織內部網路盤點 Windows Server。

2. 升級先後順序評估:

企業可依據各種類型軟體,判斷程式的重要性,優先升級重要性高者。 3. 選擇升級作業系統:

Windows Server 2003 可直接本機升級至 Windows Server 2008。若要從 Windows Server 2003 升級至 Windows Server 2012, 需先將 Windows Server 2003 升級至 Windows Server 2008, 再升級至 Windows Server 2012。

Windows Server 2003 和 Windows Server 2012 兩個版本推出時間相隔近 10 年,若直接升級至 Windows Server 2012 R2,需重新安裝系統。

4. 應用程式相容測試:

為確保原使用之軟體可於新版作業系統使用,需進行軟體相容性測試以 確認應用程式之相容性。

Microsoft 提供相容性檢測工具(Microsoft Platform Ready Test Tool, MPR Test Tool),可檢測應用程式相容性。也可以建立一個 Windows Server 2012 或 Windows Server 2008 相容性測試環境,確認應用程式相容性都沒問題後,即 可完成應用程式的移轉。

如何查看 Windows Server 版本與 Patch 更新

查看伺服器運作之 Windows Server 版本可以依下列方式操作: 開啟開始選單列→搜尋"cmd"開啟命令提示字元→輸入"winver"指令,即可查看, 流程可參考下圖1(參考範例圖1,為 Windows Server 2008 Standard SP2)。



圖 1

查看主機本身是否仍有微軟最新的更新檔案釋出,手動的方式可以按下列方式 進行操作:開啟開始選單列→選取"Windows Update"→點選"檢查更新"→選取"安 裝更新",可參考圖2範例,圖2藍色框框內文字可以查看更新的內容。



在更新的設定上,建議採取系統自身建議的"自動安裝更新",流程上請在 Windows Update 的介面選取"變更設定"→自動安裝更新即可。可參考下圖 3。

 ☆ 検査更新 型更設定 検視更新記録 還原膳藏的更新 	選擇 ₩indows 安裝更新的方式。 當您的電腦上線時, Windows 可以使用這些說定自動檢查並安裝重要更新。有可用的更新時, 您也可以在關機 之前安裝。 自動更新如何協助我?
② 更新:常見問題集	▲安史加出 下載更新,但由我來選擇是否安裝 日勤安硬那(個由我來選擇是否安裝 下載更新,但由我來選擇是否要下載及安裝它們 水邊不檢查更新(小/建議) 建議的更新 ////////////////////////////////////

圖 3

如果想確定自己本身的主機已經安裝了哪些的更新,或確保主機的更新狀態成功與否,可點選選單上的"檢視更新紀錄",在這裡可以查看到更新是否成功,另外

可以點選藍色框框部分進行日期的排序以得知目前最新的更新日期。相關範例請 參考下圖 4。

◆ 検査更新 総理論定	被視更新記錄 絵音 伊斯I 増以路初心七字結析者者更更新,学更纪险要新,转换朝口字基价更新。			
械視更新記錄	疑難排解安裝更新的問題			
還原隱藏的更新		狀態	重要性	安装▼
🔞 更新: 常見問題集 🛛 🚬	進用於 Windows Server 2008 (KB2901983) 的 Microsoft .NET Framework 4.5.2	成功	建議	2015/1/22
	KB3006226:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB2991963:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB3021674:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB3011780:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB2992611:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB890830:Windows 題意軟體移除工具 - 2015 年 1 月	成功	重要	2015/1/21
	KB3013410:Windows Server 2008 更新	成功	建議	2015/1/21
	KB3014029:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB2993958:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB3022777 : Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB3008627:Windows Server 2008 更新	成功	建議	2015/1/21
	KB3012172:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	Windows 7、Windows Vista 和 Windows Server 2008 x86 上的 Microsoft .NET Framework 4.5、4.5.1 和 4.5.2 安全性更新 (KB2978128)	成功	重要	2015/1/21
	KB3005607:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB3002885:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB3008923:Internet Explorer 7 積存安全性更新 (適用於 Windows Server 2008)	成功	重要	2015/1/21
	KB2978116:Windows Vista SP2 與 Windows Server 2008 SP2 x86 的 Microsoft .NET Framework 2.0 SP2 安全性更新	成功	重要	2015/1/21
	KB3010788:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB3013126:Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB3003743: Windows Server 2008 安全性更新	成功	重要	2015/1/21
	KB2943344:Windows Vista SP2 與 Windows Server 2008 SP2 x86 的 Microsoft .NET Framework 3.0 SP2 安全性更新	成功	重要	2014/10/28
	KB2968292:Windows Vista SP2 與 Windows Server 2008 SP2 x86 的 Microsoft .NET Framework 2.0 SP2 安全性更新	成功	重要	2014/10/28
	KB3000061:Windows Server 2008 安全性更新	成功	重要	2014/10/28

圖 4

如果對於安全性更新的漏洞有相關疑問或更多了解,可以參考網站資訊: https://technet.microsoft.com/zh-TW/library/security/ 查找相關的修補漏洞訊息,內 容包含了相對應的更新檔案編碼(參見圖5編號1)與此更新仍支援的作業系統清 單,不受此風險影響的作業軟體不會出現在清單列上,如果已經 EOS 終止支援的 作業系統也不會出現在名單列上(請見圖5編號2)。

C f Latter	t.microsoft.com/zh-TW/library,	/security/ms14-079.aspx					~	
資訊安全公告 文件庫	學習園地 下載專區 支援	社群						
								全部摺冊
₹訊安全摘要報告與公告 ₹訊安全公告	Microsoft	資訊安全公會	告 MS14-079)-中度				
MS14-085	本主顧向未接受評分 - 為這個目	主願評分						
MS14-084 MS14-083	核心模式驅動程式	中的資訊安全風險	可能會允許阻斷服務(3002885)				
MS14-082	發行日期: 2014 年 11 月 11 日	8						
MS14-081 MS14-080	版本: 1.0							
MS14-079 MS14-078	⊿提要							本頁內容
MS14-077 MS14-076	這個安全性更新可解決 Micr 網頁式攻擊的案例中,攻擊 考察注險這個思考時時度穩	rosoft Windows 中一項未公開報 者可架設一個網站,並在其中包約 個站,而且可請你用者自行並往	8告的弱點,如果攻擊者在網路共用。 合用來利用此資訊安全風險的網頁, ,一約的於注意於注障在用金點將素	上放置蓄意製作的 TrueType 字型,且使用者後續在 Win 此外,受使事的網站以及接受或存放使用者後續在 Win	ndows 檔案總管中的該處瀏覽,則 成層告的網站裡,也可能包含蓄意調	此資訊安全風險可能會允許限 製作以利用本資訊安全風險的	1断服務 (DoS)・在 内容・但是,攻撃	提要 受影響的軟體
MS14-073	当州/公理坦氏而当理約/坦州) so may instant messenger sittle mætte vætte av valuer	210 .			嚴重性等級和調
MS14-073	對於所有受支援版本的 Micr	rosoft Windows,此資訊安全更 dows 核心模式驅動程式在新入1	「新的華級為「中度」。如需更多質調 TrueTvpe 字型複素時,能正確範證」	↓ 請念問<受影響的軟體>一節。 ■列表리,進而設決比容訊安全周諦。如慶要與右關此影	· 研究全面确的管理,适参期共定管	1999全国谅的 < 爱見問簡集	(FAO) > /小師・	Windows 核心 的阻斷服務寶訂
MS14-072 MS14-071								2014-6317
MS14-070	如常有關此更新的評価資料	・ 韓参開 Microsoft 丸銀庫又件)	備號 3002005 1					資訊安全更新設
MS14-069								原財
MS14-068	▲受影響的軟體							免责聲明
MS14-067								日期
MS14-065	11 21 IEX KIE LUIZ NE MI IEU 71 IEI RII 1	些AX线球AX牛管发到影響,長10A	10年4月18日11月1日1月1日1月18日1月18日1日18日 19月1日日	· 石炭時時心的乾燥水中的支援控制, 國家國 Microso	()# 001219.2018 (0.9199.40 *			
MS14-064								
MS14-063								2
MS14-062	作業系統				最大安全性影響	彙總嚴重性等級	己取代更新	ŕ
MS14-061								
MS14-060	Windows Server 2003							
MS14-059	Windows Server 2003 Se	ervice Pack 2			阻斷服務 (DoS)	普通	MS14-058	中的 3000061
MS14-058	(3002885)							
MS14-007 MS14-056	We down 0 2002 - 0	A Falleline Constant Deate D			(0.80 (0.27) (DC)		10010.000	#++ 20000C4
MS14-055	Windows Server 2003 x6 (3002885)	94 Edition Service Pack 2			阻断服務 (D05)	首通	MS14-058	948) 3000061
MS14-054								
MS14-053	Windows Server 2003 SP (3002885)	2 for Itanium-based Systems			阻斷服務 (DoS)	首通	MS14-058	中的 3000061

Windows Server 2003 升級前的防禦措施

若於停止支援後繼續使用 Windows Server 2003 作業系統,將有諸多資安相關風險,未能如期在終止支援前完成伺服器的移轉與升級,則建議此期間採取防範方式如下,唯下列方法僅能降低資安風險,仍建議系統管理者儘快完成轉移:

1. 安裝防毒軟體:

於作業系統安裝適當的防毒軟體,並定期更新病毒碼,管理者需定期掃描 伺服器,圖6、圖7為 Microsoft 所提供的免費防毒軟體 Security Essentials 示意圖。

Microsoft Security Esser Microsoft Security Essentials	titals 飲迎使用 Microsoft Security Essentials 安裝精霊 Security Essentials 有助於改善您電腦的安全性及效能。 Security Essentials 有助於改善您電腦的安全性及效能。 Security Essentials 有拘管更新新功能和服務。因此可能需要傳送額外資訊給 Microso oft。若要讓入了解,請種類的紅種變別。安裝完成後,系統會下載最新的更新。 請按一下 [下一步] 繼續。
NT NT	<u>下-步></u> 取消 圖 6

, Microsoft Security Essentials 電驢狀態: 受保護	
 	Ø 1999 -
正在監視並保護懲的電腦。 ② 即時保護: 周啟 ③ 病毒及間諜程式定義: 同步完成	掃描選項: ⓒ 快速(Q) ⓒ 完整(E) ⓒ 自訂(C) 立即掃描(5)
及 損益詳細資料 排定的掃描: Sunday 大約 2:00 AM (快速操编) 我的操備排程 上次掃描: 9:03 AM 於 今天 (快速操猫)	
圖 7	655

2. 設定 Windows 防火牆,關閉不需要或不使用的通訊埠:

😺 Windows 防火牆	赵 進階設定 📀 🔹 🥐 😒
一般(例外)進階(服務 ICMP
網路連線設定值 Windows 防火牆已為下列所選連線啓用,若要為個別連線新增例外, 先選取它然後按「設定值」(C):	選擇在您的網際網路使用者可以存取的網路上執行的服務(S) 服務:
☑ Local Area Connection	 FTP 伺服器 Internet Mail Access Protocol Version 3 (IMAP3) Internet Mail Access Protocol Version 4 (IMAP4) Post-Office Protocol Version 3 (POP3) Telnet 伺服器
安全性記錄 您可以建立用做為疑難排解的記錄檔案。	 □ 安全網頁伺服器 (HTTPS) □ 網際網路郵件伺服器 (SMTP) □ 網頁伺服器 (HTTP) □ 遠端桌面
ICMP 使用網際網路控制訊息通訊協定 (ICMP),網路上的 電腦可以共用錯誤和狀態資訊。	
預設值 若要還原所有 Windows防火牆設定值為預設狀態, 請按 [還原成預設值]。	新增①… 编辑(①… Ⅲ除④
確定	MSEInstall (2),exe

圖 8

程式和服 【2017	務史:				_
_名偶 □UPn]					٦
□	及印表磯共用 桌面				
新增程	式(R) 新增連掛	妾埠(()	編輯(E)		

3. 密碼強度:

使用者在密碼設定的部份,可以加強密碼的強度設定以提高身份驗證的門 檻,請到「控制台」中的「使用者帳號」中設定密碼。

4. 惡意程式移除工具: 掃描惡意程式,可使用作業系統提供之掃描惡意程式工具,操作方式由開 始選單列的執行功能中輸入mrt(見圖10至圖12),也可下載Process Explorer(http://technet.microsoft.com/enus/sysinternals/bb896653)進行檢測,如 電腦裡有經過打包加工的惡意程式則該程式會呈現紫色(非淡紫)需特別注

Administrator	
🧾 管理象的伺服器	😏 我的電腦
□	☑ 控制台(C)
	● ● ● ● <td< td=""></td<>
🥙 Windows Update	(?) 說明及支援(日)
🚺 記事本	→ 搜尋(5)
遠端協助	[] 執行(<u>R</u>)
💋 遠端桌面	
会 安全性設定精靈	
WinRAR	
所有程式(P) ▶	
	💋 登出(L) 🔟 關機(U)
▶開始 」 🕑 🏈 」	圖 10
執行	<u>? ×</u>
「「」 「」 Windows	、資料夾、文件或網際網路資源的名稱, 會自動開啓。
開啓(0): 加吐	•
	確定 取消 瀏覽(B)
	圖 11

"默醒,亚曾在找到该杨乐日。 3. 你都生美知识你知识这样已教险的商会教师。
;一切報告亚列西頂測到亚且已移脉的悉息軟體。
1
<上一步(B) 下一步(B) > 取
圖 12

- Microsoft Taiwan 台灣微軟部落格, <u>http://blogs.technet.com/b/microsoft_taiwan/archive/2014/07/17/windows-server-20</u> <u>03-end-of-support.aspx</u>
- 2. http://www.ithome.com.tw/news/92982
- 3. <u>http://www.ithome.com.tw/node/83249</u>
- 4. http://news.networkmagazine.com.tw/news/2013/04/15/49056/
- 5. http://www.im.taichung.gov.tw/public/data/115020/451615502771.pdf
- 6. <u>https://www.google.com.tw/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=</u> <u>0CCoQFjAC&url=http%3A%2F%2F4c5i6s.ydu.edu.tw%2Ffront%2Fbin%2Fdownl</u> <u>oad.phtml%3FPart%3D09120028%26Nbr%3D30%26Category%3D53&ei=ITIIVd</u> <u>IPNbc8AWo_4HADw&usg=AFQjCNF4V1wTAed2V3YacYZNkc4_POEUog</u>
- 7. http://www.im.taichung.gov.tw/public/data/115020/451615502771.pdf