95 年第三季定期弱點掃瞄之說明與修補方式

一、 RealVNC 驗證方式可被規避弱點(Authentication Bypass Vulnerability)

(一) 簡要說明：

RealVNC 為廣泛使用的遠端管理工具，此工具分為 Client 與 Server 兩部份。其中 Client 藉由傳送帳號/密碼的方式，經由 Server 程式之驗證後。可進行安裝有 Server 程式系統之管理動作，其具有之權限通常為該系統之管理者權限(即 Windows 系統之 administrator 權限，或是 Unix 系統的 root 權限)，因此使用此系統之風險在於若設定之密碼不夠安全的話，將造成系統遭受誤用之風險大增。然而於 2006 年 5 月時，此軟體被發現設計之疏忽與錯誤，使得即便已設定相對安全的密碼後，仍可能讓攻擊者可輕易規避程式之驗證過程，進而以系統管理者權限管理 RealVNC server 程式所在之系統。造成嚴重後果。

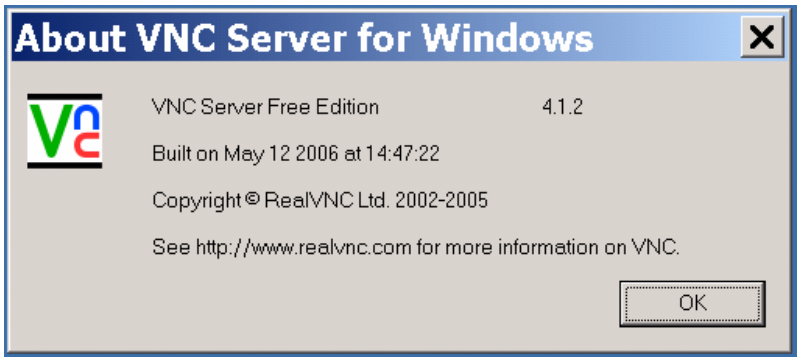
(二) 檢測方法

1. 使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 21564 進行偵測，依此判斷是否存在此弱點。若是 Nessus 系統上並無此 Plugin 存在，可能是未更新 Nessus 偵測 Plugin 造成之結果，還請執行/usr/local/sbin/nessus-update-plugins 指令更新，有關以上指令之進一步說明，可參考以下網址：http://www.nessus.org/plugins/

2. 由系統上直接檢查

若可直接登入安裝 RealVNC，亦可由系統上使用之版本直接檢查，例如以下版本為 4.1.2 版本，即為修正問題後之版本。



若為 Windows 系統，亦可由系統上之[新增移除程式]工具中驗證 VNC 之版本。其中若是 Free 版的 RealVNC 為 4.1.2 之前的版本，以及 Personal 與 Enterprise 版的 RealVNC 為 4.2.3 之前的版本的話，代表存在弱點，並且需要更新。至於 Unix Like 之系統，則請依據不同的系統套件檢查工具(如 rpm 或是 pkg_info 等等)進行檢查。

(三) 修補方式

請至官方網站(http://www.realvnc.com/)下載新版程式，並進行安裝並重新啟動即可，更新後並請再檢測是否已確實修正。

(四) 參考資料

http://lists.grok.org.uk/pipermail/full-disclosure/2006-May/046039.html

http://www.intelliadmin.com/blog/2006/05/security-flaw-in-realvnc-411.html

二、 Windows MSDTC 可讓攻擊者執行系統程式弱點或造成阻斷服務之弱點 (MS 06-018)

(一) 簡要說明：

MSDTC (Microsoft DataTransaction Coordinator)服務於 2006 年 5 月遭發現存在兩項弱點，其經由特殊設計之服務要求格式，可能導致 MSDTC 服務停止回應，造成阻斷服務情況，或是讓攻擊者得以成功入侵系統等兩項弱點。而 MSDTC 服務於 Win NT 4 與 Windows 2000 預設為啟動，而 Windows XP 及之後的系統，預設為關閉，除非自行手動啟動。而其中又以 Win NT 4 與 Windows 2000 因可能經此弱點而遭入侵成功，情況較為嚴重，而 Windows XP 與 Windows 2003 則僅可能出現阻斷服務情況。

(二) 檢測方法

1. 使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 21334 進行偵測，依此判斷是否存在此弱點。

2. 使用微軟工具檢查

使用微軟的 MBSA 工具檢查此修補程式是否已安裝，或者使用 Windows Update 工具檢查是否已安裝此修補程式。

(三) 修補方式

下載 MS06-018 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/ms06-018.mspx

若是 Windows NT 4 的系統，因不再推出修補程式，建議更換新版作業系統。

此外更新方式亦可考慮使用 Windows Update 服務進行修補，若為多台主機情況，亦可使用 SUS 或 SMS 進行修補。

(四) 參考資料

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0034

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1184

三、 Windows 路由與遠端存取服務存在可讓攻擊者執行任意程式弱點 (MS06-025)

(一) 簡要說明：

Windows 路由與遠端存取服務(Routing and Remote Access Service，簡寫為 RRAS)之用途在於讓 Windows 系統得以運作為網路閘道器一般，另外此服務亦提供遠端存取之功能(涵蓋之前之 Remote Access Service 之功能)，例如可讓使用者藉由電話撥接的方式存取遠端之 Windows 系統，就如同彼此實體連線一般，使用者可經由此服務，於遠端之 Windows 系統上執行寄送電子郵件、讀取檔案或列印等。此服務為 Windows 2000、XP 與 2003 內建之服務。

由於此服務之連線管理程式(Remote Access Connection Manager，簡稱為RASMAN)與 Remote Procedure Call (RPC)之溝通介面存在緩衝區溢位之弱點，使得攻擊者藉由傳送特殊設計之 RPC 相關溝通封包，可望入侵存在弱點之 Windows 系統。依據微軟對此弱點之風險分析，此弱點可讓匿名之使用者(不具 Windows 系統帳號)取得 Windows 2000 SP4 (包含 SP3 與之前)或 Windows XP SP1 系統之管理者權限。而對於 Windows XP SP2 與 Windows 2003 系統，則需先具備系統之帳號方可利用此弱點。

(二) 檢測方法

1. 使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 21696 進行偵測，依此判斷是否存在此弱點。

2. 使用微軟工具檢查

使用微軟的 MBSA 工具檢查此修補程式是否已安裝，或者使用 Windows Update 工具檢查是否已安裝此修補程式。

(三) 修補方式

下載 MS06-025 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/ms06-025.mspx

若為多台主機情況，可考慮使用 SUS、WSUS 或 SMS 進行修補。

(四) 參考資料

http://www.kb.cert.org/vuls/id/814644

http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-2371

四、 Windows 系統 Server 服務可導致攻擊者得執行任意程式弱點 (MS06-035)

(一) 簡要說明：

Windows 中提供 Mailslot 通訊方式，其藉由 SMB 傳送協定傳送兩種形式之 SMB 封包，一為 TCP 形式，一為 UDP 形式。前者提供連線導向之封包，後者用以傳送非連線導向之封包(例如廣播封包)。本弱點出現的情況在於 Windows 系統上用以管理 Server Message Block (SMB)封包的驅動程式 SRV.SYS，由於其處理方式疏失，可讓攻擊者藉由特殊設計的 SMB 封包觸發弱點，造成嚴重後果。

本弱點遭利用後，導致的後果在於可讓攻擊者在無任何權限的前提下，得以獲得系統上"System"之權限，得以完全掌控受駭系統，諸如竊取機密資料或利用系統執行任意程式，如攻擊其他系統或刪除系統上重要檔案等。

依據微軟對此弱點之風險分析，此弱點屬於嚴重層級。另存在此弱點的系統包含有 Windows 2000 SP4 (包含 SP3 與之前)、Windows XP SP1 與 SP2 及 Windows 2003 與 Windows 2003 SP1 系統。

(二) 檢測方法

1. 使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 22034 進行偵測，依此判斷是否存

在此弱點。

2. 使用微軟工具檢查

使用微軟的 MBSA 工具檢查此修補程式是否已安裝，或者使用 Windows Update 工具檢查是否已安裝此修補程式。

(三) 修補方式

下載 MS06-035 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

或者使用 Windows Update 服務更新，可於 IE 瀏覽器中的「工具」中選擇「Windows Update」，另外 Windows NT 4.0 Workstation、Windows NT 4.0 Server 與 Windows 2000 SP2 及 Windows 2000 SP3 皆已超過微軟之維護時限，務必變更到更新的版本方可修補此弱點。

若為多台主機情況，可考慮使用 SUS、WSUS 或 SMS 進行修補。

最後由於本弱點係藉由 TCP port 445 進行攻擊，因此若無必要，請使用防火牆阻擋外界對此通訊埠之連線。

(四) 參考資料

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1314
http://www.tippingpoint.com/security/advisories/TSRT-06-02.html
http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

五、 Windows 系統 Server 服務可導致攻擊者得執行任意程式弱點 (MS06-040)

(一) 簡要說明：

同為 Windows 系統 Server 服務出現之弱點，但此弱點與先前出現之弱點(MS 06-035)不同，屬於不同之弱點，為微軟內部自行發現之弱點，此弱點在於當 Server 服務於處理特殊設計之 MS RPC 訊息時，結果可能導致無系統任何權限之攻擊者得以獲得系統上”System”之權限，完全掌控受駭系統，諸如竊取機密資料或利用系統執行任意程式，如攻擊其他系統或刪除系統上重要檔案等。值得特別留意的是，本弱點雖與 MS 06-035 同樣為出現在 Server 服務之弱點，但兩者屬於不同之兩項弱點，亦即同樣之 Server 服務先後出現兩項重大弱點，並需同時安裝各自之修補程式方可消弭弱點。

依據微軟對此弱點之風險分析，此弱點屬於嚴重層級。另存在此弱點的系統包含有 Windows 2000 SP4 (包含 SP3 與之前)、Windows XP SP1 與 SP2 及 Windows 2003 與 Windows 2003 SP1 系統。

另據 2006/8/16 張貼於 Security Focus 的消息指出，名為 W32.Warbot 的蠕蟲被發現嘗試利用此弱點大量進行感染攻擊。

(二) 檢測方法

3. 使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 22194 進行偵測，依此判斷是否存在此弱點。

4. 使用微軟工具檢查

使用微軟的 MBSA 工具檢查此修補程式是否已安裝，或者使用 Windows Update 工具檢查是否已安裝此修補程式。

(三) 修補方式

下載 MS06-040 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

或者使用 Windows Update 服務更新，可於 IE 瀏覽器中的「工具」中選擇「Windows Update」，另外 Windows NT 4.0 Workstation、Windows NT 4.0 Server 與 Windows 2000 SP2 及 Windows 2000 SP3 皆已超過微軟之維護時限，務必變更到更新的版本方可修補此弱點。

若為多台主機情況，可考慮使用 SUS、WSUS 或 SMS 進行修補。

最後由於本弱點係藉由 TCP port 139 或 TCP port 445 進行攻擊，因此若無必要，請使用防火牆阻擋外界對此通訊埠之連線。

此外須特別留意的是，微軟證實當安裝此修補程式的系統為 Windows 2003 SP1 的 32 位元版本時，則有可能後續執行需大量記憶體之程式出現失敗之情況，此問題請參考：

http://support.microsoft.com/kb/924054/

(四) 參考資料

http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

http://www.kb.cert.org/vuls/id/650769

http://www.securityfocus.com/bid/19409

****

* **Revision**: 2006/7/10 Version 1.0，沿用前季之第四與第五項弱點，新增

* MS 06-25 弱點為第三項。

* 2006/7/25 Version 1.1，新增第四項弱點(MS 06-035)。

* 2006/8/21 Version 1.2，新增第五項弱點(MS 06-040)。

****