94 年第四季定期弱點掃描之說明與修補方式

一、 Windows SMB 協定可讓攻擊者執行系統程式弱點(896422—MS 05-027)

(一) 簡要說明：

Windows 主機使用 Server Message Block (SMB)協定，或稱為 Common Internet File System (CIFS)的協定，使 windows 主機可以將另一 Windows 主機目錄檔案當成是本機上的目錄檔案使用，即所謂的網路芳鄰分享。而這個協定亦可以用於 Internet 網段，即位於不同網段的 Windows 主機也可使用此協定進行目錄檔案的分享(假如傳送過程中未有其他的網路設備阻擋時)或是遠端管理功能用途。

今年(2005 年)6 月中，微軟之 SMB 協定被發現存在嚴重弱點，結果將導致攻擊者得以經由此弱點取得系統的完全控制權，由於 SMB 協定所使用的通訊埠為 TCP port 139 或是 TCP port 445，因此若是 Windows 主機存在此弱點且未有防火牆阻擋來自 Internet 對這些 ports 的連線，將導致來自遠端的攻擊者得以經由此弱點入侵此系統，並獲得完全之掌控權。

本弱點於微軟的本身的弱點編號為 MS 05-027，而 CVE 的弱點編號為 CAN-2005-1206，本弱點的嚴重程度為 Critical，為十分嚴重之弱點。

影響平台：

除 Windows 98, Windows 98 SE 與 Windows ME 外，所有的 Windows 作業系統系列皆存在此問題(如 Windows 2000, Windows XP 與 Windows 2003)，至於 Windows NT 4.0 由於已不再推出修補程式，微軟網站上並無此系統的說明，可能亦存在此問題。

(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 18502 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 MS05-027 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/MS05-027.mspx

若是 Windows NT 4 的系統，因不再推出修補程式，建議更新至較新版本。

或者使用 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。另在安裝修補程式之外，建議使用防火牆阻擋來自 Internet 對內部系統(含內部網路或是 DMZ 區的系統)之 TCP port 139 與 445 的存取，以防此弱點遭受利用。

(四) 參考資料

微軟官方說明文件：

http://www.microsoft.com/technet/security/bulletin/ms05-027.mspx

CVE 對此弱點之說明文件：

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1206

二、 Windows Plug and Play 服務可讓攻擊者執行系統程式弱點(899588—MS 05-039)

(一) 簡要說明：

Windows 使用 Plug and Play 服務用來偵測系統安裝的硬體，譬如於 Windows 系統上接上滑鼠時，系統將偵測該滑鼠，載入必要的驅動程式以讓使用者使用。本項服務於 2005 年 8 月遭發現存在 Buffer overflow 的弱點，結果導致遠端攻擊者可經由傳送特定格式之封包給 TCP port 445，讓攻擊者取得系統上的完整權限，或者產生阻斷服務(DoS)攻擊之情況，另已發現有自動化的電腦蠕蟲(例如 Zotob worm)針對此弱點進行自動攻擊，實為嚴重之問題，此外本機上的非管理者權限使用者亦可能經由此弱點取得管理者之權限。受本項弱點影響之平台包含 Windows 2000, Windows XP 與 Windows 2003，而 Win 98 與 Win ME 並無此弱點，至於 Windows NT 4.0 由於已不再推出修補程式，微軟網站上並無此系統的說明，可能亦存在此問題。

(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 19408 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 MS05-039 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/MS05-039mspx

若是 Windows NT 4 的系統，因不再推出修補程式，建議更新至較新版本。或者使用 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。另在安裝修補程式之外，建議使用防火牆阻擋來自 Internet 對內部系統(含內部網路或是 DMZ 區的系統)之 TCP port 445 的存取，以防此弱點遭受利用。

(四) 參考資料

微軟官方說明文件：

http://www.microsoft.com/technet/security/bulletin/ms05-039.mspx

CERT 弱點說明文件：

http://www.kb.cert.org/vuls/id/998653

三、 Windows Printer Spooler 服務可讓攻擊者執行系統程式弱點(896423—MS 05-043)

(一) 簡要說明：

Windows 主機上的 Printer Spooler 服務為系統開機時便啟動，直到關機才停止。此服務本身為一執行檔(spoolsv.exe)，該服務的用途在於管理系統上的列印工作，包含擷取印表機驅動程式，載入驅動程式，執行列印工作或列印工作排程等。本項服務於 2005 年 8 月亦遭發現存在 Buffer Overflow 的弱點，若存在此弱點且遠端攻擊者藉由吸引系統使用者連結至特殊設計的惡意印表機，則在與該印表機的連結過程中，該系統便可能被驅動 Buffer Overflow 的情況，導致攻擊者可經此取得該系統上的權限，並可執行系統程式，本弱點於微軟的本身的弱點編號為 MS 05-043，而 CVE 的弱點編號為 CAN-2005-1984，本弱點的嚴重程度為 Critical，為十分嚴重之弱點。

影響平台：

除 Windows 98, Windows 98 SE 與 Windows ME 外，所有的 Windows 作業系統系列若未安裝修補程式，皆存在此問題(如 Windows 2000 SP4 或之前, Windows XP SP2 或之前與 Windows 2003)，至於 Windows NT 4.0 由於已不再推出修補程式，微軟網站上並無此系統的說明，可能亦存在此問題。

(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 19407 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 MS05-043 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/MS05-043.mspx

若是 Windows NT 4 的系統，因不再推出修補程式，建議更新至較新版本。或者使用 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。另在安裝修補程式之外，建議使用防火牆阻擋來自 Internet 對內部系統(含內部網路或是 DMZ 區的系統)之 TCP port 139 與 445 的存取，以防此弱點遭受利用。

此外亦可藉由關閉此服務或是移除此程式的方式修正，不過這樣將導致系統無法進行列印工作(不論是本機上的印表機或是遠端印表機)，關閉方式可參考：

http://www.kb.cert.org/vuls/id/220821

(四) 參考資料

微軟官方說明文件：

http://www.microsoft.com/technet/security/bulletin/ms05-043.mspx

CERT 弱點說明文件：

http://www.kb.cert.org/vuls/id/220821

四、 Windows NetWare Client 端服務可讓攻擊者執行系統程式弱點(899589—MS 05-046)

(一) 簡要說明：

Microsoft 上的 Netware 的 Client 端服務套件遭發現存在可讓攻擊者從遠端執行系統上任意程式的嚴重弱點，本項弱點存在於 Windows 2000 SP4 (尚未安裝 SP4 的 Windows 2000 系統亦存在此弱點)、Win XP SP1 與 Win XP SP2，Windows 2003 與 Windows 2003 SP1。

存在此弱點的系統，也可能包含已不再推出修補程式的系統。欲判斷所使用的系統是否仍在 Microsoft 的服務週期內，請參考

http://support.microsoft.com/default.aspx?scid=fh;[ln];lifecycle

或者當使用檢測工具(MBSA 或是 Nessus)判斷存在弱點時，即很有可能存在弱點。

由於存在本項弱點的 Netware Client 端服務，預設上並不會啟動，唯有當使用者自行啟動此服務的情況才會啟動，也才可能存在此弱點。

(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 20006 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

1. 安裝修補程式

下載 MS05-046 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/MS05-046.mspx

或者使用 Windows Update 服務進行修補，若為多台主機情況，亦可使用 WSUS，SUS 或 SMS 進行修補。

2. 停用 Netware Client 端服務

另外一個解決此弱點的方式為停用此服務，尤其若是單位內並沒有 Netware 系統的情況，在 Windows 的系統上並不需要此服務。停用的方式為在[控制台]的[網路與撥號連線]中選擇該主機的網路介面，檢視其中的內容，並將 Netware client 端的用戶端服務(Client Service for Netware)移除。此外若是該系統上存在多個網路介面，若欲停用此服務，則各個網路介面皆須設定。

(四) 參考資料

微軟官方說明文件：

http://www.microsoft.com/technet/security/bulletin/ms05-046.mspx

五、 Windows MSDTC 及 COM+可讓攻擊者執行系統程式弱點(kb902400—MS 05-051)

(一) 簡要說明：

MS 05-051 弱點的修補程式修正數項新發現的弱點，包含有 MSDTC (Microsoft Transaction Coordinator)弱點、COM+弱點以及 TIP (Transaction Internet Protocol)弱點。前兩者可能讓攻擊者取得系統上管理者權限，並得以執行系統上的程式，而最後一項可能導致阻斷服務攻擊。所有除了 Win 98、Win 98 SE 以及 Win ME 外的 Windows 系統，若未安裝此項弱點的修補程式，即有可能存在此弱點。

存在此弱點的系統，包含已不再推出修補程式的系統。欲判斷所使用的系統是否仍在 Microsoft 的服務週期內，請參考

http://support.microsoft.com/default.aspx?scid=fh;[ln];lifecycle

或者當使用檢測工具(MBSA 或是 Nessus)判斷存在弱點時，即很有可能存在弱點。

(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 20008 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。

3. 由系統之登錄值進行檢查

於執行中輸入 regedit 指令後，由其中的尋找工具尋找以下的數值(902400)是否存在，若存在代表此系統已安裝修補程式，否則為未安裝修補程式。

(三) 修補方式

下載 MS05-051 的修補程式，網址為：

http://www.microsoft.com/technet/security/Bulletin/MS05-051.mspx

或者使用 Windows Update 服務進行修補，若為多台主機情況，亦可使用 WSUS、SUS 或 SMS 進行修補。另在安裝修補程式之外，建議使用防火牆阻擋來自 Internet 對內部系統(含內部網路或是 DMZ 區的系統)非必要通訊埠的連線，並僅開放必要之 ports，以防此弱點遭受利用。

(四) 參考資料

微軟官方說明文件：

http://www.microsoft.com/technet/security/bulletin/ms05-051.mspx

****
* **Revision**: 2005/10/07 v1, 沿用前一季其中三項弱點項目，為本季的第一至第
* 三項
* 2005/10/17 v1.1, 新增第四及第五項弱點項目
*
****