95 年第一季定期弱點掃瞄之說明與修補方式

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。

本項弱點存在於微軟之 SMB 協定，弱點遭利用的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 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。此服務為系統開機時便啟動，直到關機才停止。本項服務於 2005 年 8 月遭發現存在 Buffer Overflow 的弱點，若系統存在此弱點且遠端攻擊者藉由吸引該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。

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. 使用弱點掃瞄軟體—Nessus 檢測

使用 Nessus 掃瞄軟體，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

三、 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. 使用弱點掃瞄軟體—Nessus 檢測

使用 Nessus 掃瞄軟體，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

四、 phpMyAdmin 存在可讓攻擊者以 Web 服務權限執行任意程式與讀取任意檔案弱點

(一) 簡要說明：

phpMyAdmin 為以 PHP 程式語言撰寫，為 Web 介面之 MySQL 資料庫管理工具，為 Open Source 軟體套件。由於 Web 介面與簡易性，因此對於不清楚 MySQL 操作指令的人士而言，可以較具親和力的介面管理 MySQL 資料庫，此軟體如一般 CGI 程式相同，若程式本身對於使用者(或是攻擊者)於 Web 介面上輸入的字元未有適當的過濾機制時，即有可能導致攻擊者得以 Web 伺服器的權限執行系統上的任意程式或是讀取任意檔案。此問題尤其對於系統上權限設定不安全時最為嚴重，例如管理者可能疏忽以致重要之設定檔，可讓具有 Web 服務的權限者進行修改，如此當攻擊者經由 CGI 程式弱點而獲得 Web 服務權限後，即可能導致系統無法正常運作。甚至配合系統上存在的其他弱點，可能得以提升權限至管理者等級，如此系統將不再受到信任，也無法再使用。

不幸的是，phpMyAdmin 亦存在若干未適當過濾字元的弱點，結果即可能出現以上的情況，因此使用此軟體時，應有適當之權限管理(比方限制可以使用的連線來源)，並且應使用最新版本，尤其當重大弱點發布後，務必加以更新以消弭問題。而 phpMyAdmin 目前最新之版本為 2.7.0-pl2。

(二) 檢測方法

1. 使用弱點掃瞄軟體—Nessus 檢測

使用 Nessus 掃瞄軟體，並且使用 Plugin ID 15478、15948、17221 進行偵測，依此判斷是否存在此弱點。

2. 直接查詢軟體版本

由程式使用介面中即可看出所用之版本，若是所用之版本並非最新版本，則應加以更新。

(三) 修補方式

依據 phpMyAdmin 官方網站對於舊版本弱點的建議修補方式，皆為下載新版本並更新，因此若存在弱點請至官方網站(http://www.phpmyadmin.net/)下載新版軟體並安裝，安裝方式一般僅需修改設定檔中與 MySQL 資料庫之連結帳號與密碼等相關資訊即可。若更新上有問題時，請特別留意以下網頁中關於軟體運作需求部份是否符合：http://www.phpmyadmin.net/documentation/。

(四) 參考資料

phpMyAdmin 相關弱點文件網址：

http://www.phpmyadmin.net/home_page/security.php

****

* **Revision**: 2005/12/30 v1, 沿用前一季兩項弱點項目，為本季的第一至第二項，第三項為本季新增弱點項目

* 2006/1/10 v1.1, 再沿用前一季第一項弱點項目，使為本季的第一項，原三項弱點項目標號依序增加

****