94 年第三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、AWStats 軟體之輸入驗證弱點

(一) 簡要說明

AWStats 為一免費的即時記錄檔分析軟體，可用來做 Web 紀錄檔的分析，甚至是 FTP 或 Mail 紀錄檔之分析，其中在版本低於 6.4 的情況下，存在未適當驗證使用者輸入值的弱點，結果使得使用者得以輸入特殊的值，經由該軟體執行特定行為。出現弱點的原因，在於此軟體對於使用者經由 HTTP 協定送給 awstat.pl 的 URL request 中所出現的"configdir"或"logfile"並未加以過濾檢查，以致 awstat.pl 出現預期外之行為。

攻擊者經由此弱點，將可能以 Web 服務的執行權限執行系統上的程式，或是以 Web 服務的權限讀取系統上的檔案內容。

(二) 偵測方式

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 14347 及 16189 進行偵測，依此判斷是否存在此弱點。

2. 直接由系統檢查所用 AWStats 之版本

依據不同的作業系統，檢查該系統上所安裝的 AWStats 版本會有所不同，請參考所用的作業系統文件。另可直接於 Command Line 模式下執行 awstats.pl，其執行產生的結果中，第一行會出現目前程式的版本訊息。

3. 使用 Web 瀏覽器檢查

可使用一般的 Web 瀏覽器，針對安裝有 AWStats 軟體的 Web Server，執行 awstats.pl(通常位於 http://www.example.com/cgi-bin/awstats.pl)，傳回的網頁內容中，含有版本資訊，可依此檢查。

(三) 解決方式

請升級到 6.4 的版本，或者不需要此軟體的情況下，考慮移除。

(四) 參考資料

http://securityfocus.com/bid/10950

http://securityfocus.com/bid/12270

三、疑似遭入侵之 IIS 偵測

(一) 簡要說明

IIS 為 Windows 系統預設使用的 Web server，幾乎大部分使用 Windows 系統作為 Web 伺服器的管理人員皆會選擇使用 IIS，而 IIS 也是所有 Web server 中佔有率第二的套件。本項偵測試圖判斷提供服務的 IIS server 中，是否存在異常的

可執行程式，例如位於 IIS scripts 目錄下的 cmd.exe 或是 root.exe 執行程式，前者一般為 Windows 系統目錄下的 cmd.exe 程式遭複製至 scripts 目錄，後者一般為感染 CodeRed 而遭複製系統 cmd.exe 程式於此，並變更檔名為 root.exe。至於其他的惡意程式，例如 cmd.asp 或 upload.asp 等，通常都是攻擊者入侵 IIS server 後，會選擇置放於系統上的，其中 cmd.asp 用途類似於 cmd.exe，用以執行系統指令，而 upload.asp 則用以傳送檔案至系統上。雖然攻擊者經由 Web 介面執行以上程式的權限為 Web 服務之權限，但仍可能洩漏系統上的機密資訊，並且攻擊者亦可能利用其他方式提昇權限(如利用其他弱點)。需注意的是，攻擊者不侷限於放置上述之程式，甚至程式亦可能以不同的名稱顯示。

因此若是 Web 所用目錄下(一般為 scripts 與 msadc 目錄)存在異常的執行程式(非為系統管理人員安裝使用之程式)，很有可能是 IIS server 遭受入侵，並被置放特定執行程式以供攻擊者利用。

(二) 偵測方式

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 11003 進行偵測，依此判斷是否存在此弱點。

2. 直接由系統檢查

可直接於 IIS 目錄下檢查是否存在異常執行程式或 DLL 檔案。

(三) 解決方式

於檢查過程中發現之檔案，確定為異常檔案，請予刪除。若不確定是否為異常檔案，建議先行移至 IIS 目錄之外(例如放於 c:\temp\目錄下)，若驗證並不影響原有功能，再刪除該異常檔案。

技術服務中心偵測後之結果，將註明被發現主機上的異常程式名稱，可依此進行修正，格式如下：

說明	原本之檔案名稱	顯示之檔案名稱
範例 1	cmd.exe	scripts/az.exe
範例 2	cmd.exe	scripts/cmd1.exe scripts/az.exe
範例 3	upload.asp	msadc/upload.asp
範例 4	radmin	scripts/admdll.dll scripts/raddrv.dll

偵測結果中，其中原本的檔案名稱代表經判斷原始之檔案名稱，而顯示之檔案名稱則為實際於系統上發現之檔案名稱。例如範例 1，該執行檔案原始之名稱經判斷為 cmd.exe，但經更名為 az.exe，並置放於 scripts 目錄下；而範例 2 中，同樣的執行檔案—cmd.exe 則被複製 2 份於系統上，分別為 cmd1.exe 與 az.exe，亦即這兩個檔案的名稱皆有變更，並同樣置放於 scripts 目錄下；範例 3 則為類似範例 1 的情況；最後的範例 4 則為 radmin 此遠端管理套件中的兩個 DLL 檔案(admdll.dll 與 raddrc.dll 被偵測到)被發現存在於 scripts 目錄下。故在收到偵測結

果時，請依顯示之名稱，檢查系統上是否存在該檔案，若有則請依本節—解決方式之第一段的方式處理。

Ps. IIS server 目錄上的執行程式皆應確認正常，預期外的執行程式不應置放於該目錄。

(四) 參考資料

http://www.nessus.org/plugins/index.php?view=single&id=11003

****

* 本季於 9 月初新增之兩項掃瞄項目 *

* 掃瞄項目與解決方法說明如下 *

****

四、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

五、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(sploolsv.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

****

* **Revision**: 2005/07/28 v1, 涵蓋一到三項弱點之說明

* 2005/09/09 v1.1, 增加四到五項弱點之說明

****