94 年第二季定期弱點掃描之說明與修補方式

一、Windows 主機系統管理者帳號未設定密碼弱點

1. 簡要說明

本項弱點於 92 年第三季掃描中已測過，本季掃描此項的原因在於此項弱點經測試後，仍有若干主機存在此問題，需要修正，以下部分內容節錄該次掃描的原始內容，作為此次文件之說明。

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。雖然 SMB 協定具有相當的便利性，但設定不夠完善的 Windows 主機(如密碼設定不夠安全或是未設定密碼)常讓外界使用者經此網路芳鄰分享，洩漏區域網路內相關檔案或系統上的機密資訊，甚至讓網路駭客完全控制該部主機。

2. 檢測方式

(1) 使用 Nessus 檢驗

使用 Nessus 掃描軟體，並且使用 Plugin ID 10394 進行偵測，依此判斷是存在管理者未設定密碼之問題。

(2) 使用網芳連線檢查

使用網芳直接針對可能存在問題的主機進行連線，若是輸入帳號”administrator”後，不需輸入密碼即可登入，代表該系統的管理者帳號未設定密碼保護。

3. 修補方式

(1) 阻擋非必要的網芳分享：

特別是對於來自 Internet 的連線請求，建議與以阻擋。阻擋方式為使用防火牆設定僅有需要的 ports 才開放(如 IIS 所使用的 port 80)，而關閉網芳或 Windows 遠端管理所使用的 ports(如 port 135、137-139、445)。另不論是否關閉上述的 ports，仍需設定安全之密碼。

(2) 密碼設定方式：

建議將 Windows 系統上的帳號設定成符合密碼設定原則的密碼。

(a) NT 4：

可直接同時按下 Ctrl+Alt+Del，在其中可以輸入欲變更密碼之帳號，輸入舊密碼後即可輸入新密碼。或是從<開始>**à**<程式集>**à**<系統管理工具(公用)>**à**<網域使用者管理員>**à**<本機使用者與群組>，在其中選取使用者並設定新密碼即可。

(b) Windows 2000 或以上

可直接同時按下 Ctrl+Alt+Del，在其中可以輸入欲變更密碼之帳

號，輸入舊密碼後即可輸入新密碼。或是從<開始>à<程式集>à<系統管理工具>à<電腦管理>à<本機使用者與群組>，在其中的使用者選取欲變更密碼之帳號，設定密碼即可。若是 Windows 2000 professional 版，則其<系統管理工具>位置與 Windows 2000 server 不同，請由<控制台>中選取。或者直接在<控制台>中選取<使用者與密碼>設定系統上帳號的密碼。

4. 參考資料

http://www.sans.org/top20/#w5

二、Microsoft SMTP 弱點

1. 簡要說明

Microsoft SMTP server 於 93 年第四季遭發現存在嚴重的緩衝區溢位問題，並可能導致攻擊者於該系統上執行任意程式，此弱點於 93 年第四季掃描中已進行掃描，此次將對此問題進行複測。關於此弱點的其他資訊，請參考該季之說明文件，或是參考 MS04-035 弱點的說明。

2. 檢測方式

(1) 使用 Nessus 檢查

使用 Nessus 編號 15464 的 Plugin ID 檢查。以此判斷有無設定密碼。

(2) 使用 Windows Update 網站檢驗

使用 IE 工具中的"Windows Update"選項連結至微軟的系統更新服務，由其中的檢視並安裝更新檔可供檢查，並可安裝修補程式。

(3) 使用 MBSA 進行掃描

使用 MBSA 進行掃描，檢查是否未安裝修補程式。

3. 修補方式

下載 MS04-035 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx

或者參考該季之說明文件，或者使用 SUS 或 SMS 進行修補。

4. 參考資料

http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx

三、HTTP dangerous method (PUT, Delete)弱點

1. 簡要說明

HTTP dangerous method 弱點在於 HTTP 提供經由 HTTP 協定的方式，可以針對 Web server 進行檔案上傳與刪除，如此若是 Web server 權限設定不當時，將可能發生網頁出現不預期的修改情況，一般而言此過大的權限預設是關閉的，但仍有可能出現不預期的情況而開啟。此弱點於 92 年的第四季已進行掃描，但因發現仍有單位經此弱點而造成網頁遭竄改，因此於本季再次進行掃描。

2. 檢測方式

使用 Nessus 編號 10498 的 Plugin ID 檢查。以此判斷有無設定密碼。

3. 修補方式

針對微軟 IIS 系統的修補方式，該次掃描文件上已有詳細說明，內容如下：

請完成以下三個步驟以預防不預期的 HTTP PUT：

(1) 如果該網站不需使用 WebDAV (Web Distributed Authoring and Versioning)，建議將其關閉。目前已知 FrontPage 會使用 WebDAV，若不確定是否使用 WebDAV，建議可先行關閉，若發現網站因此無法正常運作再將其啟用。欲關閉 WebDAV，請執行 regedit，於

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters

加入以下 registry value:

Value name: DisableWebDAV

Data type: DWORD

Value data: 1

需重新啟動 IIS 以使用新設定，若要再次啟用 WebDAV 則將其值設為 0。

(2) 執行 Internet 服務管理員，檢查系統上所有的 Web 站台的權限，在選取的 Web 站台上按右鍵選內容，點選主目錄，確認寫入權限未被核取，對於其下的所有虛擬目錄也請一併檢查。

(3)強化 Web 所在資料夾 (一般為 %SystemDrive%\Inetpub\wwwroot) 存取權限，該資料夾對於 Internet 來賓帳戶 (IUSR_MachineName) 或 Everyone 等帳戶，通常僅需提供讀取權限即可。

4. 參考資料

http://www.icst.org.tw/template/ncert/iiacnsc.htm

四、SNMP 預設 Community Name 弱點

1. 簡要說明

SNMP 代表 Simple Network Management Protocol，被廣泛使用來做遠端管理與監控網路設備，如設定網路組態與監控流量等。並使用 Community name 作為溝通憑證，但因若干網路設備預設使用的 Community name，因此攻擊者可以藉由嘗試這些名稱，試圖獲取網路設定組態與流量資訊，或是針對賅網路設備或電腦主機進行管理。故需變更原先之名稱以規避此弱點，此弱點於 92 年的第四季已進行掃描，本次掃描將再進行複測。此次將針對預設之管理 Community name – private 進行掃描，檢查是否有存在此名稱的情形。

2. 檢測方式

使用 Nessus 掃描軟體，並且使用 Plugin ID 10264 進行偵測，依此判斷有無弱點存在。另外若是回應的 Community name 為 public，雖然僅是用來

傳遞訊息用途，仍應進行修改，以避免資訊洩漏。

3. 修補方式

參考該次掃描的修補文件，內容如下：

如果不需使用 SNMP，建議將其關閉。如果需要使用到 SNMP，請設定一組較複雜之 Community，並設定防火牆或路由器阻擋 SNMP 所使用之 TCP Prot 161 及 UDP Port 161/162。

(1) 以 Cisco IOS 為例，若欲關閉 SNMP，則執行

no snmp-server

若欲取消某一 SNMP Community，則執行

no snmp-server community string

例如欲取消 public 這一個 Community，則執行

no snmp-server community public

若欲設定為某一 SNMP Community，則執行

snmp-server community string ro|rw

例如欲設定 strong_community 有可寫入權限，則執行

snmp-server community strong_community rw

(2) Windows 系統不需使用 SNMP 者，請於服務中停用 Simple Network Management Protocol，或直接透過新增移除程式將其移除。

(3) RedHat Linux 請執行下列指令關閉 snmp：

service snmpd stop

chkconfig snmpd off

其他設備 SNMP 設定方法請尋求設備廠商協助

4. 參考資料

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/cfr_1g10.htm#1034652

http://www.cert.org/advisories/CA-2002-03.html