一、Apache chunked 弱點

1. 簡要說明

Apache web server 當收到以 Chunked 方式編碼的資料，因為無適當計算接收 buffer 大小的機制，以致發生 buffer overflow 或是 race condition 的情況，結果會造成攻擊者可以執行系統上任意程式的弱點。這個弱點發生在 Apache 1.2.2 即以前的版本，或是 Apache 1.3 到 1.3.24 的版本，或 Apache 2.0 到 2.0.36 的版本。

另針對這個問題攻擊的電腦病毒據傳也在網路上散佈。

2. 檢測方式

可自行下載 Eeye Digital 的 Apache chunk 弱點的偵測工具進行偵測，網址為：
http://www.eeye.com/html/Research/Tools/RetinaApacheChunked.exe
依據結果可判斷有無弱點。

3. 解決方案

修正的方式可分成升級 Apache 版本，或是安裝各作業平台維護廠商或團體所提供的修補程式。

升級的話請升級到 Apache 1.3.26 或之後的版本，或是 Apache 2.0.39 或之後的版本。下載網址為：http://www.apache.org

請安裝各作業平台所提供的修補程式，如 RedHat linux，請執行 up2date 指令進行預設安裝 apache 的弱點修補，若是使用 FreeBSD 的話，請移除舊版的 Apache，並從 port 裡更新新版 Apache，port 位址為：/usr/port/www/apache13/、/usr/port/www/apache13-modssl/，或/usr/port/www/apache2/。至於其他平台的安裝請依據參考資訊進行修補，網址為：

http://online.securityfocus.com/bid/5033/solution/
http://www.kb.cert.org/vuls/id/944335

4. 參考資料

http://www.kb.cert.org/vuls/id/944335
http://www.cert.org/advisories/CA-2002-17.html

二、未正確設定權限之 FrontPage Server Extension (FPSE)

1. 簡要說明

FPSE 為微軟所提供之遠端網站管理程式，管理者可在有安裝 FrontPage 的遠端機器上，直接修改 IIS 伺服器上之網頁。然常有網站管理者疏忽或為求方便，未正確設定存取權限，因而使惡意使用者可在未經授權的情況下，任意修改該 IIS 伺服器上之網頁。

2. 檢測方法

若有安裝 FrontPage，可試著直接以 FrontPage 連接該 IIS 伺服器，若不需認證便可成功連上，則該伺服器存在此問題。若無安裝 FrontPage，則可在命令提示字元下，執行 telnet www.yourorg.tw 80，輸入 “POST /_vti_bin/_vti_aut/author.dll

HTTP/1.0”，若回應訊息中可看到“HTTP/1.1 200 OK”，則通常便代表此伺服器安裝有不需認證之 FPSE；若回應訊息中可看到“HTTP/1.1 401 Access denied”則通常代表此伺服器安裝有 FPSE，且已正確設定認證；若出現其他訊息，則應該無此問題。也可直接檢測目錄權限，Windows NT 4.0 可檢視 C:\InetPub\wwwroot_vti_bin\ 其下目錄及檔案的權限，Windows 2000 可檢視 C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\isapi 其下目錄及檔案的權限，若使用者 Everyone 對此目錄擁有存取權限，則通常便代表此伺服器有此弱點。

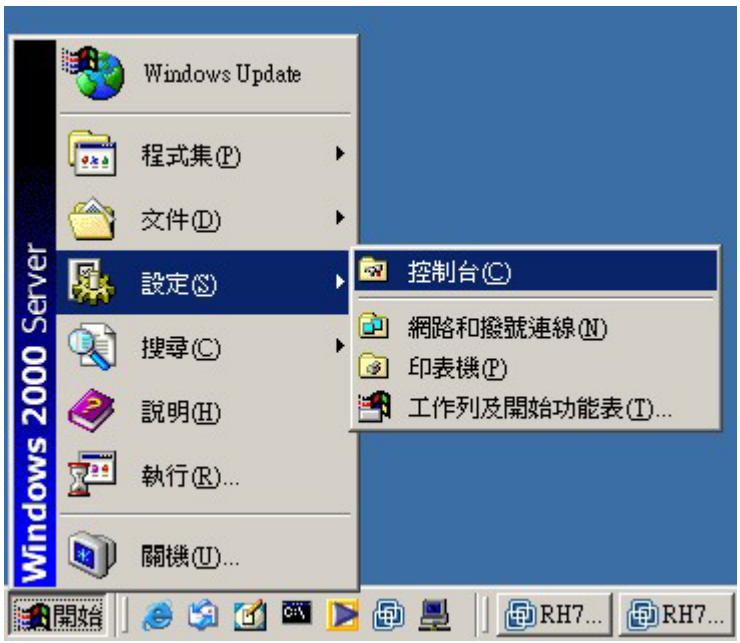
3. 解決方案

若此系統並不需使用 FPSE，請將其移除。

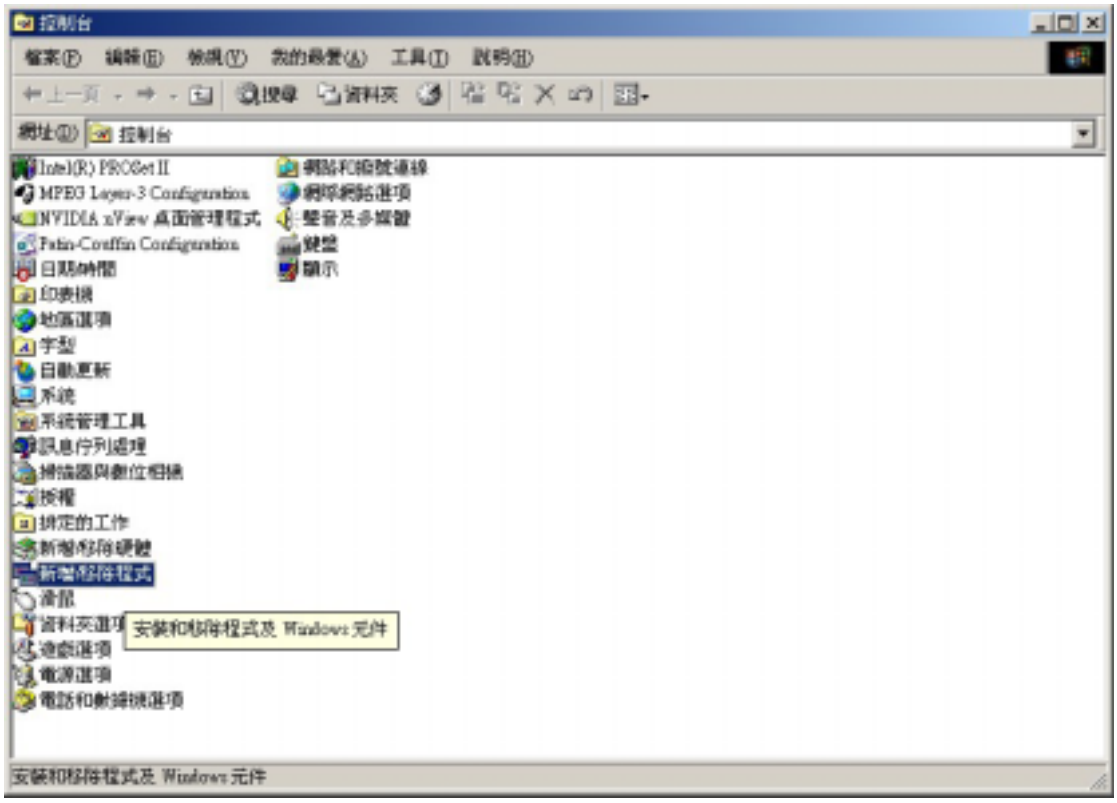
若此系統需使用 FPSE，請設定適當權限，將網頁所在目錄 (C:\Inetpub\wwwroot) 及 FPSE 使用目錄 (2 所提到之目錄) 之 Everyone 權限設成只允許“讀取及執行、清單資料夾內容與讀取”。系統上不要有不需要之帳號，必須之帳號則需設定強健之密碼。

3.1 Windows 2000 下移除 FPSE 的步驟。

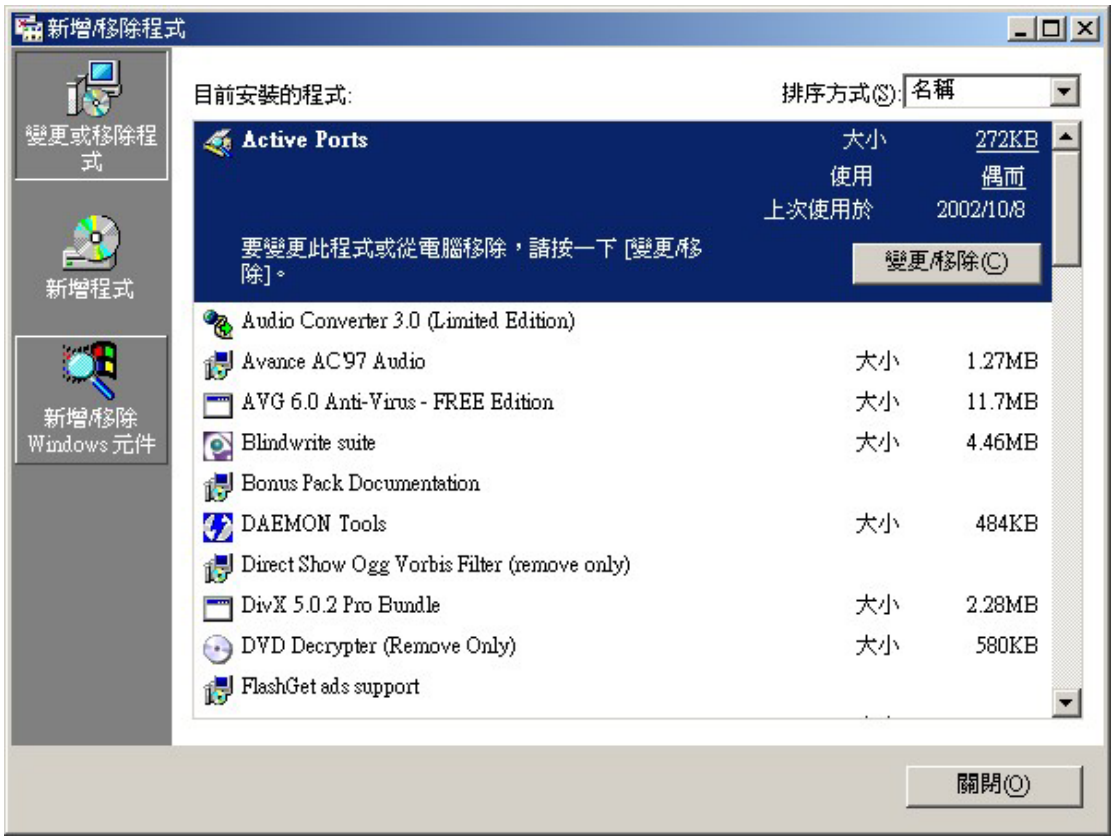
3.1.1. 開始功能表 -> 設定 -> 控制台



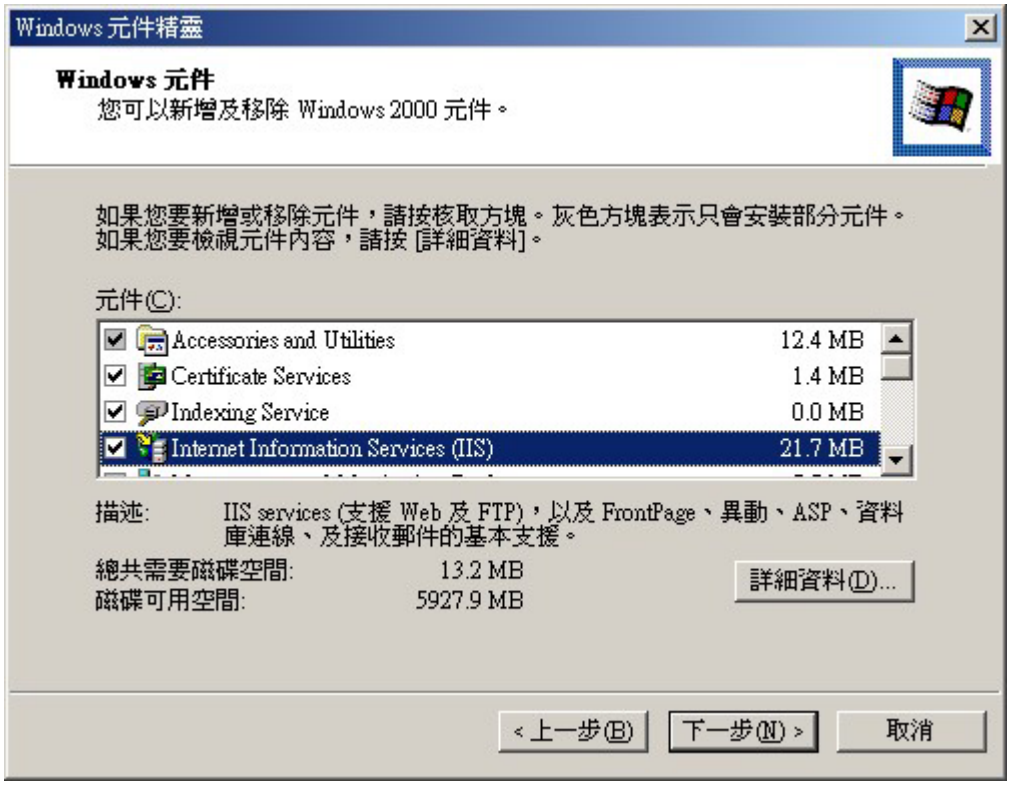
3.1.2. 選取 新增/移除程式



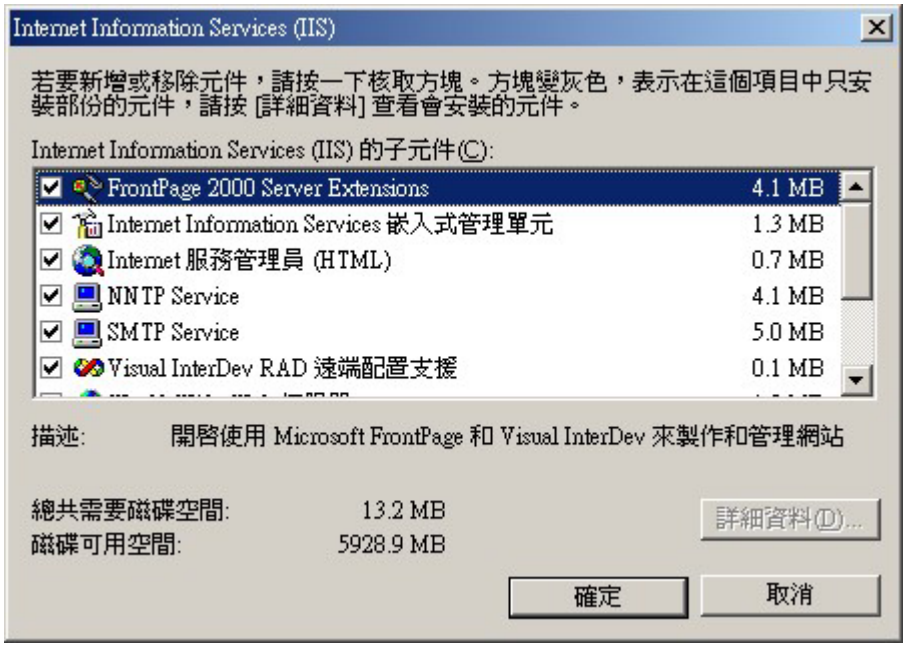
3.1.3. 點選 新增/移除 Windows 元件



3.1.4. 選取 Internet Information Services (IIS)，點選 詳細資料

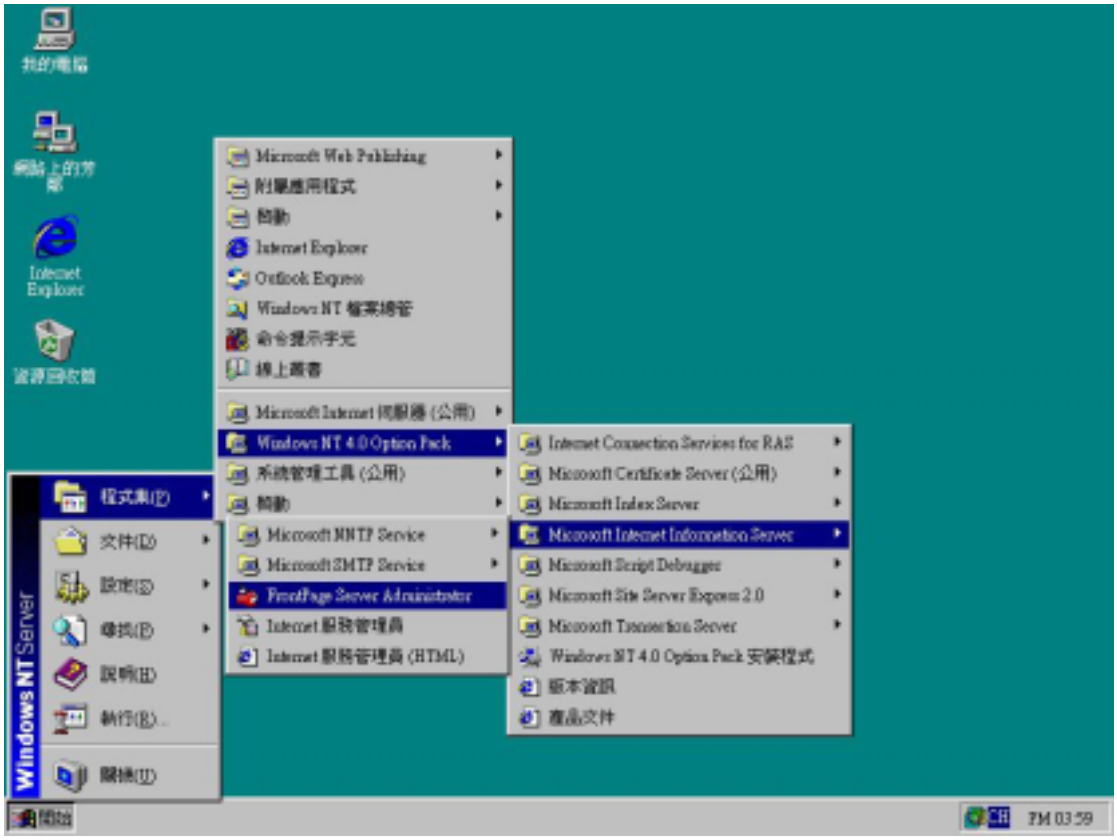


3.1.5. 取消 FrontPage 2000 Server Extensions 上之 V

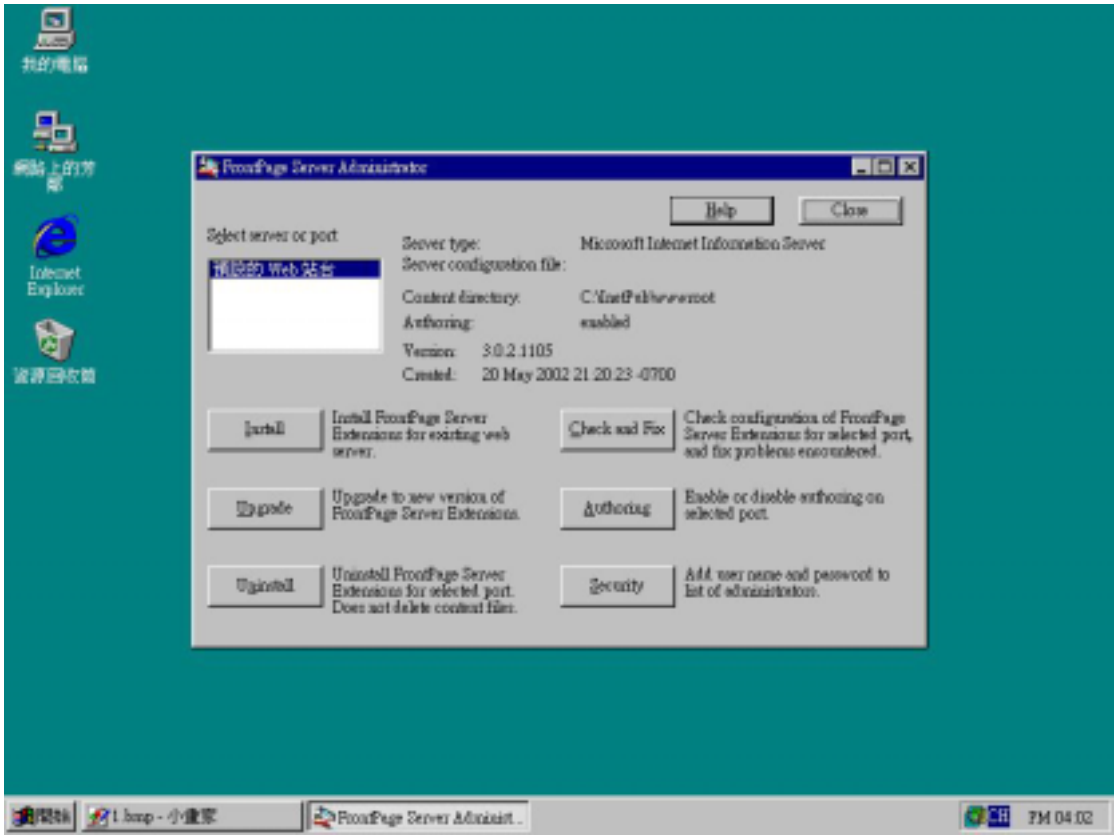


3.2 Windows NT 4.0 下移除 FPSE 的步驟。

3.2.1. 開始功能表 -> Windows NT 4.0 Option Pack -> Microsoft Internet Information Server -> FrontPage Server Administrator



3.4.2 若要移除請選 Uninstall。



三、OpenSSL 弱點

1. 簡要說明

OpenSSL 為一可免費取得之 SSL 實作，大多數 Unix 系統利用其來提供 Web Server (Apache)之 SSL 功能，藉以提供加密與伺服器認證之安全通訊。然在 OpenSSL 0.9.6d 及 0.9.7-beta2 之前的版本，存在緩衝區溢位的弱點，攻擊者可利用此弱點獲取系統上的 shell，進而執行任意命令。

在大約 91/9/12 左右，網路上流傳一隻稱為 Apache/mod_ssl Worm (Slapper worm)的電腦蠕蟲，會透過使用 OpenSSL 的 Apache 伺服器感染網路上的主機，並進而達到分散式阻斷服務 (DDoS) 攻擊。

2. 檢測方法

可下載 http://cert.uni-stuttgart.de/advisories/openssl-sslv2-master/openssl-sslv2-master.c 做自我檢測，需以 gcc -lcrypto openssl-sslv2-master.c -o openssl-sslv2-master 編譯。

若已受到 Apache/mod_ssl Worm 攻擊，可下 ls -al /tmp/ 看在此目錄下是否找到 .uubugtraq、 .bugtraq.c、 .bugtraq、 .unlock、 .cinik.uu、 .cinik.c、 .cinik.go、 .cinik.goecho 及 .cinik 等檔案。Linux 可下 netstat -anp --inet 看看是否有開啟 UDP port 2002、4156、1978 及 1812，TCP port 1052 等。亦可以 ps -auxw 查看是否有 .bugtraq、 .cinik 及 .unlock 等 process 正在執行。以 crontab -l -u apache 檢查使用者 apache 的 crobtab 裡是否有排程以上 process。

3. 解決方案

升級至最新版之 OpenSSL，可至http://www.openssl.org下載，在寫這份文件之時，最新穩定版本為 0.9.6g。亦可安裝廠商所提供之修正程式，RedHat Linux 可至http://www.redhat.com/apps/support/errata/ 下載，下載完後以 rpm -Fvh *.rpm 安裝修正程式。若在步驟 2 中檢測出已遭受攻擊，則可下載 chkrookit 以清除此電腦蠕蟲 (http://www.chkrootkit.org/)。

4. 參考資料

http://www.cert.org/advisories/CA-2002-23.html
http://www.chkrootkit.org/

附錄：

Windows 2000/NT + IIS 5.0/4.0 修正說明，完成下列動作後，將可修補大部分 Windows 及 IIS 的漏洞。

1. 安裝 Service Pack:

Windows 2000 Service Pack 3 (2002/8):
http://www.microsoft.com/downloads/release.asp?releaseid=40842

Windows NT 4.0 Service Pack 6a (2000/1):
http://www.microsoft.com/downloads/release.asp?ReleaseID=17624

Windows NT 4.0 Service Pack 6a Security Roll-up Package(2001/7/26):
http://www.microsoft.com/ntserver/nts/downloads/critical/q299444/default.asp

2. 安裝 IIS 安全修正 MS02-062(2002/10/30):
IIS 5.0:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=43296

IIS 4.0:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=43566

3. 安裝 IE 安全修正 (若在 server 上會執行 IE):
IE 6 SP1(2002/9/25)
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=43216

4. 檢查遺漏之修正程式：
以下步驟請依序執行。
4.1.執行 Windows Update，安裝檢查到的修正程式，可連上網址 http://windowsupdate.microsoft.com。
4.2.Windows 2000 可執行 Microsoft Baseline Security Analyzer
此工具可檢查目前 Windows 尚未安裝哪些重大修正程式，並提供部分增進安全之設定，可至下列網址下載：
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsahome.asp
4.3.Windows NT 可執行 HFNetChk，可至下列網址下載：
http://www.microsoft.com/downloads/release.asp?releaseid=31154
此工具可檢查目前 Windows 尚未安裝哪些重大修正程式。建議以 hfnetchk -z -nosum 執行，檢查時出現 Note 者為提供資訊用；出現 Warning 者可能為已安裝該修正程式，但版本號碼不同；出現 Patch NOT Found 則一般代表並未安裝此修正程式，執行時亦可加 -v 參數以顯示較詳細資訊。但由於其原來係針對英文版所設計，部份檢查結果會有誤判，當檢查結果出現 Q123456 尚未安裝時，可於新增/移除程式中驗證是否的確未安裝。