94 年第一季定期弱點掃描之說明與修補方式

一、Windows WINS server 可供入侵以執行任意程式弱點

1. 簡要說明

Windows Internet Naming Service (WINS)為用來作為將 IP addresses 對應到 NetBIOS 電腦名稱用途，用途類似於 DNS server。而於 Windows NT server SP 6a, NT Terminal Server 4.0 SP6, Windows 2000 Server SP3 與 SP4，及 Windows Server 2003 上，因其未正確檢驗於 WINS 封包裡的電腦名稱欄位，結果可能產生 Buffer Overflow 的弱點，藉由傳送特殊的封包給 WINS server 所用的 TCP port 42 上，可能因此弱點而讓遠端攻擊者得於系統上執行任意程式。或是造成 DoS 攻擊情況，由於 WINS server 預設為系統 Local System 權限啟動，故攻擊者可望獲得的權限亦為 Local System 權限，因此為相當嚴重的問題。

2. 檢測方式

(1) 使用 Nessus 檢驗

使用 Nessus 掃描軟體，並且使用 Plugin ID 15970 進行偵測，依此判斷有無弱點存在。

(2) 由本機直接檢查

由系統上的控制台的新增移除程式的變更或移除程式項目中檢查有無編號 870763 的 Hotfix 安裝在系統上，或者從 registry key 中的適當位置檢查該編號的 Hotfix 是否存在，例如 Windows 2000 系統的路徑為：
HKLM\SOFTWARE\Microsoft\Update\Windows 2000\SP5
若是其他系統則位置有所不同，此外亦可從 registry key 編輯工具的尋找功能找尋有無以上 Hotfix 存在。

(3) 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，其中的”檢視並安裝更新檔”可供檢查，並可安裝修補程式。

3. 修補方式

請依據 MS04-045 的修補建議安裝修補程式，
http://www.microsoft.com/technet/security/bulletin/ms04-045.mspx

4. 參考資料

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0567
http://www.microsoft.com/technet/security/bulletin/ms04-045.mspx

二、MySQL server 未設定管理者權限弱點

1. 簡要說明

MySQL 為一 Open Source 的資料庫軟體，因其免費且效能亦不錯，故為廣泛使用的資料庫軟體，而在安裝時，因其預設並未設定管理者的密碼，若是系統

管理者安裝後，並未設定密碼即予使用，且未使用防火牆阻擋對 MySQL server 使用的 port (預設為 3306)的連線，則攻擊者可由遠端登入 MySQL server，修改、新增、刪除資料庫上的資料，甚至是從遠端非法管理此資料庫軟體。也由於資料庫上存在的資料多為單位內的機密資料，或是會員帳號/密碼等資料。故未設定管理者密碼所造成的後果自是相當嚴重。

2. 檢測方式

(1) 使用 Nessus 檢查

使用 Nessus 編號 10481 的 Plugin ID 檢查。以此判斷有無設定密碼。

(2) 使用 MySQL 指令檢查

可於安裝有 MySQL server 與 MySQL client 的主機上執行以下指令：

> mysql -u root

若系統並未顯示任何錯誤訊息即進入 MySQL 的提示符號 *mysql*>，及代表 MySQL server 並未設定管理者密碼，例如：

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 139 to server version: 4.1.7-nt

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

反之若系統出現權限問題以致無法登入訊息，代表系統無此弱點。另外若欲測試 MySQL 的主機非為本機，則請將上述指令改為：

>mysql -u root --host=target_ip

其中的 target_ip 代表安裝有 MySQL server 的主機。

最後若系統無 mysql 指令，代表此系統應無安裝 MySQL client 套件，可於安裝後再使用。

3. 修補方式

於安裝有 MySQL server 的 Unix 系統下以 root 身分登入，並執行以下指令設定，其中 your_password 請改成選定的密碼，並且該密碼應符合密碼複雜度原則。

mysqladmin password your_password

此外亦請考慮使用防火牆或是路由器的連線管控機制，控制可直接連結此 MySQL server 的來源，例如禁止來自 Internet 對此 3306 TCP port 的連線能力。

4. 參考資料

http://www.nessus.org/plugins/index.php?view=single&id=10481

http://dev.mysql.com/doc/

三、phpBB 低於 2.0.11 版本存在可供執行任意程式弱點

1. 簡要說明

phpBB 為使用 PHP 語言寫成的 Web 論壇套件，為一免費且設定與使用皆容易的套件。phpBB 於過去至今，曾被發現若干弱點，其中最新的弱點出現在

2.0.11 前的版本，較 2.0.11 為舊的版本存在有 script injection 的弱點，結果可讓攻擊者以 Web server 的權限執行系統上的任意程式，若是系統上的 Web server 的執行權限為管理者權限，則攻擊者有可能獲得因此弱點獲得系統上的管理者權限，如此將更提升風險。

2. 檢測方式

(1) 使用 Nessus 檢查

使用 Nessus 編號 16200 的 Plugin ID 檢查。以此判斷有無設定密碼。

(2) 使用瀏覽器檢查

使用瀏覽器開啟安裝有 phpBB 的網頁—index.php，若是網頁內容中出現 Powered by phpBB *version*，若是其中的版本低於 2.0.11，代表需要更新。

3. 修補方式

安裝 phpBB 2.0.11 以後(含 2.0.11)的版本以修補此問題。

4. 參考資料

http://www.securityfocus.com/bid/10701

phpBB 官方網站： http://www.phpbb.com/

四、IIS ASP ISAPI filter 存在 Buffer Overflow 弱點

1. 簡要說明

ASP 為 Windows 推出用以提供 Active Web page 的網頁之程式語言，類似於 PHP 語言，其於 2002 年被發現存在有 Buffer Overflow 的弱點，攻擊者藉由觸發存在於 IIS Web server 上的 ASP ISAPI filter 解譯引擎的 Buffer Overflow 的弱點，有可能獲得系統上執行 IIS server 的權限(預設為 Local System)，結果將導致攻擊者可以此權限執行系統上的任意程式。

受影響平台:

IIS 4.0

IIS 5.0

IIS 5.1

ps. 雖然此弱點已存在超過兩年，但因其嚴重性高，故於此季掃描中加入此項。

2. 檢測方式

(1) 使用 Nessus 檢驗

使用 Nessus 掃描軟體，並且使用 Plugin ID 10935 進行偵測，依此判斷有無弱點存在。

(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. 修補方式

參考 MS 02-018 的弱點修補說明：

http://www.microsoft.com/technet/security/bulletin/ms02-018.mspx
或者使用 Windows Update 網站安裝。

另外於 2002 年以後才推出的 Windows 系統 Service Pack (如 Windows 2000 SP)皆包含此問題的修正程式，亦可藉安裝 Service Pack 修正此問題。

4. 參考資料

http://www.microsoft.com/technet/security/bulletin/ms02-018.mspx

五、LSASS 弱點(MS 04-011)複測

技服中心曾於去年第 3 季掃描中針對 LSASS 弱點(MS 04-011) (2004 年第 3 季的第 1 項)進行掃描，因其嚴重性與攻擊程式已存在許久的情況，易出現受害情況，因此於本季中再次針對此弱點進行偵測，以期發現潛在問題。詳細說明與修補方式請參考該季之說明文件。或者參考以下網址進行修正：

http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx