93 年第 4 季偵測弱點之說明與修補方式

一.MySQL 身分驗證弱點

1. 簡要說明：

MySQL 是現行常用的 open source 資料庫之一，效率也不錯。目前(2004.10 底)MySQL.com 建議的穩定發行版本是 MySQL 4.1.x，MySQL 5.0.x 則是還在測試階段。在 MySQL 4.1.1、4.1.2、5.0.0 的身分驗證機制存在個弱點，惡意使用者可以透過傳送特殊字串的方式，不需要輸入正確的使用者帳號與密碼，即可繞過 MySQL 的身分驗證機制，取得 MySQL 資料庫的管理控制權。

2. 受影響版本：

MySQL 4.1.1

MySQL 4.1.2

MySQL 5.0.0

3. 檢測方式：

3.1 檢查系統上 MySQL 的版本

查詢系統上 MySQL 版本的指令如下，

[root@xxx root]# mysqld –V，

或是[root@xxx root]# mysqld –version，

若是系統回應訊息 MySQL 的版本爲 4.1.1、4.1.2、5.0.0，表示 MySQL 資料庫會受到該弱點的影響。

3.2 用 Nessus 檢查主機是否有 MySQL 身分驗證弱點

檢查系統是否存在 MySQL 身分驗證弱點，可用 Nuessus 做外部掃描，掃描的 plugin ID 爲 12639。

4. 弱點修正：

4.1 MySQL 版本 4.1.x

若系統上所安裝的 MySQL 版本爲 4.1.x，請將 MySQL 的版本升級至 4.1.x 的最新版本，目前(2004.10 底)4.1.x 最新版本爲 4.1.7，管理者可至 MySQL 的官方網站(www.mysql.com)，下載最新版本的 MySQL 資料庫，MySQL 4.1.x 的下載網址爲，http://dev.mysql.com/downloads/mysql/4.1.html，管理者請依自己的需求

下載原始檔或是執行檔進行更新的動作。

在更新前請管理者務必將資料庫先行備份，以及詳細閱讀過 MySQL 版本更新所做的修改，參考網址爲，http://dev.mysql.com/doc/mysql/en/News-4.1.x.html。

在 Linux 的環境下，管理者可下載 rpm 套件進行更新，目前 MySQL 最新版本 rpm 套件爲 MySQL-server-4.1.7-0.i386.rpm，安裝升級的指令如下，

[root@xxx root]# rpm –Uvh MySQL-server-4.1.7-0.i386.rpm

4.2 MySQL 版本 5.0.x

目前 MySQL 版本 5.0.x 尚未修補此弱點，建議不要使用 MySQL 版本 5.0.x，除了因爲 MySQL 版本 5.0.x 尚未修補此弱點外，此版本的 MySQL 是 MySQL.com 的新產品，目前還在測試階段，所以穩定性較不足，實驗性質較重。

5. 參考資料：

securityfocus.com Bugtraq 10654 - MySQL Authentication Bypass Vulnerability

http://www.securityfocus.com/bid/10654

MySQL 4.1 Downloads

http://dev.mysql.com/downloads/mysql/4.1.html

MySQL Manual | C.2 Changes in release 4.1.x (Production)

http://dev.mysql.com/doc/mysql/en/News-4.1.x.html

二. OpenSSL 緩衝區溢位問題

1. 簡要說明：

OpenSSL 爲一可免費取得的 SSL 實作，大多數 Unix 系統利用其來提供 Web Server 之 SSL 功能，藉以提供加密與伺服器認證之安全通訊。在 OpenSSL 版本 0.9.6k 或 0.9.7c 之前(不包括版本 0.9.6k 與 0.9.7c)存在緩衝區溢位的弱點，惡意的使用者可利用此弱點對系統進行阻斷式服務攻擊，或是透過該弱點執行任意的命令。

2. 受影響版本：

OpenSSL 0.9.6k 之前(不含 0.9.6k)

OpenSSL 0.9.7c 之前(不含 0.9.7c)

3. 檢測方式：

3.1 檢查 OpenSSL 版本

查詢系統上 OpenSSL 版本的指令如下，

[root@xxx root]# openssl version

若系統回應的 OpenSSL 版本資訊爲 0.9.6k 或 0.9.7c 之前的版本，則 OpenSSL 會受到該弱點影響。

檢查 OpenSSL 的版本有個地方需要注意，在 Red Hat Linux 的環境下，若管理者是使用 rpm 的方式直接升級 OpenSSL，則上述的檢查方式就不適用，即使在安裝了最新的 OpenSSL 最新 rpm 套件，系統也會回應 OpenSSL 0.9.7a Feb 19 2003。請改用以下的方式查詢 OpenSSL 版本，

[root@xxx root]# rpm –q openssl

不同 Red Hat 發行版本，修補後的 OpenSSL rpm 的版本資訊皆不同，更詳細的資訊請參考 4.弱點修正。

3.2 用 Nessus 檢查主機是否有 OpenSSL 緩衝區溢位問題

檢查系統是否存在 OpenSSL 緩衝區溢位問題，可用 Nuessus 做外部掃描，掃描的 plugin ID 爲 11875。

4. 弱點修正：

4.1 下載安裝最新版本 OpenSSL 原始檔

目前(2004.10 底)OpenSSL 最新版本爲 openssl-0.9.7e，請至 www.openssl.org 下載並安裝。

4.2 Red Hat Linux 環境

Red Hat 有提供更新後的 OpenSSL rpm 套件，請依據不同的版本的 Red Hat Linux 下載適當的 OpenSSL rpm 套件，相關更新資料請參考，

http://rhn.redhat.com/errata/RHSA-2003-291.html

http://rhn.redhat.com/errata/RHSA-2004-121.html

Red Hat Linux 7.1：openssl-0.9.6-19.src.rpm

ftp://updates.redhat.com/7.1/en/os/SRPMS/openssl-0.9.6-19.src.rpm

http://updates.redhat.com/7.1/en/os/SRPMS/openssl-0.9.6-19.src.rpm

Red Hat Linux 7.2：openssl-0.9.6b-35.7.i386.rpm

ftp://updates.redhat.com/7.2/en/os/i386/openssl-0.9.6b-35.7.i386.rpm

http://updates.redhat.com/7.2/en/os/i386/openssl-0.9.6b-35.7.i386.rpm

Red Hat Linux 7.3：openssl-0.9.6b-35.7.i386.rpm

ftp://updates.redhat.com/7.2/en/os/i386/openssl-0.9.6b-35.7.i386.rpm

http://updates.redhat.com/7.2/en/os/i386/openssl-0.9.6b-35.7.i386.rpm

Red Hat Linux 8.0：openssl-0.9.6b-35.8.i386.rpm

ftp://updates.redhat.com/8.0/en/os/i386/openssl-0.9.6b-35.8.i386.rpm

http://updates.redhat.com/8.0/en/os/i386/openssl-0.9.6b-35.8.i386.rpm

Red Hat Linux 9：openssl-0.9.7a-20.2.i386.rpm

ftp://updates.redhat.com/9/en/os/i386/openssl-0.9.7a-20.2.i386.rpm

http://updates.redhat.com/9/en/os/i386/openssl-0.9.7a-20.2.i386.rpm

安裝指令爲，

[root@xxx root]# rpm –Fvh openssl-version.i386.rpm

其中 version 是指不同版本 Linux 所適用的不同 OpenSSL rpm 套件版本。

5. 參考資料：

securityfocus.com Bugtraq 8732 - OpenSSL ASN.1 Parsing Vulnerabilities

http://www.securityfocus.com/bid/8732

OpenSSL 官方網站

http://www.openssl.org

RHSA-2003:291-11

http://rhn.redhat.com/errata/RHSA-2003-291.html

RHSA-2004:121-04

http://rhn.redhat.com/errata/RHSA-2004-121.html

三. Windows 工作排程器(Task Scheduler)弱點

1. 簡要說明：

在某些版本 windows 作業平台發現其工作排程器(Task Scheduler)有緩衝區問題，惡意的使用者可以利用該弱點在系統上執行任意的程式碼。

2. 受影響平台：

Microsoft Windows 2000 Service Pack 2

Microsoft Windows 2000 Service Pack 3

Microsoft Windows 2000 Service Pack 4

Microsoft Windows XP

Microsoft Windows XP Service Pack 1

3. 檢測方式：

檢查系統是否存在工作排程器(Task Scheduler)問題，可用 Nuessus 做外部掃描，掃描的 plugin ID 爲 13852-MS Task Scheduler vulnerability。

4. 弱點修正：

安裝 Microsoft Windows Windows 最新的修補程式。

4.1 Windows Update

請管理者連上 Windows Update 的網站，檢查系統是否有尚未安裝的修補程式。

4.2 手動下載安裝此弱點的修補程式

(1) Microsoft Windows 2000

此弱點 Microsoft Windows 2000 的下載網址爲，
http://www.microsoft.com/downloads/details.aspx?displaylang=zh-tw&FamilyID=BBF3C8A1-7D72-4CE9-A586-7C837B499C08

(2) Microsoft Windows XP

此弱點 Microsoft Windows XP 的下載網址爲，

http://www.microsoft.com/downloads/details.aspx?displaylang=zh-tw&FamilyID=8E8D0A2D-D3B9-4DE8-8B6F-FC27715BC0CF

5. 參考資料：

Microsoft Security Bulletin MS04-022 中文版

http://www.microsoft.com/taiwan/security/bulletin/MS04-022.mspx

Microsoft Security Bulletin MS04-022 英文版

http://www.microsoft.com/technet/security/bulletin/ms04-022.mspx

KB841873：Windows 2000 安全性更新

http://www.microsoft.com/downloads/details.aspx?displaylang=zh-tw&FamilyID=BBF3C8A1-7D72-4CE9-A586-7C837B499C08

KB841873：Windows XP 安全性更新

http://www.microsoft.com/downloads/details.aspx?displaylang=zh-tw&FamilyID=8E8D0A2D-D3B9-4DE8-8B6F-FC27715BC0CF

四.Microsoft SMTP 弱點

1. 簡要說明：

在某些版本 windows 作業平台或是安裝 Microsoft Exchange Server 的作業平台發現其 SMTP 有緩衝區溢位問題，惡意的使用者可以利用該弱點在系統上執行任意的程式碼。

2. 受影響平台：

Microsoft Windows Server 2003

Microsoft Exchange Server 2003 on Microsoft Windows Server 2003

Microsoft Exchange Server 2003 Service Pack 1 on Microsoft Windows Server 2003

Microsoft Exchange Server 2003 on Microsoft Windows 2000 Service Pack 3

Microsoft Exchange Server 2003 on Microsoft Windows 2000 Service Pack 4

3. 檢測方式：

檢查系統是否存在 Microsoft SMTP 弱點，可用 Nuessus 做外部掃描，掃描的 plugin ID 爲 15464-MS SMTP Vulnerability。

4. 弱點修正：

4.1 系統沒有安裝 Microsoft Exchange Sever 2003

請使用 Windows Update 功能將 Windows Server 2003 更新至最新狀態，或是手動下載安裝此弱點的修補程式，KB885881 - Windows Server 2003 安全性更新，下載網址爲，
http://www.microsoft.com/downloads/details.aspx?familyid=d7767455-1ca0-49ea-8f71-76da5d451a07&displaylang=zh-tw。

4.2 系統有安裝 Microsoft Exchange Sever 2003

請手動下載並安裝 Microsoft Exchange Server 2003 此弱點的修補程式，KB885882 - Exchange 2003 安全性更新，
http://www.microsoft.com/downloads/details.aspx?familyid=313BEC77-0845-46D4-BB43-06C792ADB2EA&displaylang=zh-tw

5. 參考資料：

Microsoft Security Bulletin MS04-035 中文版

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

Microsoft Security Bulletin MS04-035 英文版

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

KB885881：Windows Server 2003 安全性更新

http://www.microsoft.com/downloads/details.aspx?familyid=d7767455-1ca0-49ea-8f71-76da5d451a07&displaylang=zh-tw

KB885882：Exchange 2003 安全性更新

http://www.microsoft.com/downloads/details.aspx?familyid=313BEC77-0845-46D4-BB43-06C792ADB2EA&displaylang=zh-tw

五. W32.Spybot 網蟲

1. 簡要說明：

W32.Spybot 是隻會透過網路感染的網蟲，它包含許多種傳播機制，包括透過點對點的分享軟體，如 KaZaA。Spybot 除了感染主機外，還會在主機上安裝後門程式，以便惡意使用者可遠端遙控被感染主機。

2. 受影響平台：

Microsoft Windows 作業系統

3. 檢測方式：

3.1 檢查系統上是否有異常程式或機碼

W32.Spybot 在感染受害主機後，會將自己複製到%System%\sysmsvc.exe，%system%是指系統磁區，若使用者將 Windows 安裝於 C:\，W32.Spybot 則會將自己複製到 C:\syssmsvc.exe。

除了複製自己至%system%外，W32.Spybot 還會在以下的 registry 路徑加入機碼"MsWindows SysDate" = "sysmsvc.exe"，

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

HKEY_CURRENT_USER\Software\Microsoft\OLE

HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control\Lsa

這可確保 W32.Spybot 在每次系統重新啓動後會再次被執行。

3.2 用 Nessus 檢查主機被 W32.Spybot 感染

檢查系統是否被 W32.Spybot 感染，可用 Nuessus 做外部掃描，掃描的 plugin ID 爲 15520-w32.spybot.fcd worm infection。

4. 弱點修正：

(1) 將系統離線

將系統離線可以避免在作清除動作時，系統又再次被網蟲感染。

(2) 關閉「系統還原」(適用 Windows Me/XP)

「系統還原」是 Windows Me/XP 預設的功能，此功能原來是用來備份系統的，但是可能會一併將電腦上的病毒、病蟲或特洛伊木馬備份起來。所以在進行清除前請先將「系統還原」功能關閉，關閉的方式請參考，

如何關閉或啓用 Windows XP「系統還原」

http://service1.symantec.com/SUPPORT/INTER/traditionalchinesekb.nsf/tw_docid/20020517102945932

如何關閉或啓用 Windows Me「系統還原」

http://service1.symantec.com/SUPPORT/INTER/traditionalchinesekb.nsf/tw_docid/20020517101224932

(3) 更新防毒程式的病毒定義檔

請在一台乾淨的機器上下載防毒軟體的最新病毒定義檔，並安裝在受感染主機上。

(4) 用防毒程式掃描並移除惡意程式

(5) 刪除機碼

在編輯 registry 可能會對系統造成不可預期的危害，所以請務必小心執行並先備份 registry，請在[開始]->[執行]，打入 regedit，並點選[OK]，此時電腦會出現 registry 編輯程式，請至下面路徑，

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

HKEY_CURRENT_USER\Software\Microsoft\OLE

HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control\Lsa

刪除"MsWindows SysDate" = "sysmsvc.exe"。

5. 參考資料：

Symantec 安全威脅 - W32.Spybot.FCD

http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.fcd.html