92 年第四季 偵測弱點之說明修補方式

一、Microsoft RPC DCOM 弱點 - MS03-039

1. 簡要說明

微軟的 RPCSS (Remote Procedure Call - 遠端程序呼叫) 含有緩衝區溢位的弱點，攻擊者可以利用此弱點在未經授權的情況下，透過網路於有弱點的系統上執行任意程式碼，或對系統發動阻斷服務攻擊。著名的 MSBlast(疾風)即利用微軟 RPC 弱點進行傳播，微軟於 Advisory MS03-026 中針對其 RPC 弱點作了修補，然而修補並不完整，因此又釋出 MS03-039 修補程式。Windows NT/2000/XP/2003 均受此弱點影響，建議儘早安裝此修補程式。

2. 檢測方法

可於本機上執行新增移除程式，檢查是否安裝了 Hotfix KB824146 (Q824146)；亦可下載微軟所提供的掃描程式透過網路進行掃描

http://www.microsoft.com/downloads/details.aspx?displaylang=zh-tw&FamilyID=13AE421B-7BAB-41A2-843B-FAD838FE472E

安裝完後會將掃描程式放置於 %ProgramFiles%\KB824146Scan 資料夾下，執行 KB824146Scan.exe host 即可掃描單一主機，執行 KB824146Scan.exe network_address/cidr_mask 即可掃描整個子網路，如欲掃瞄 192.168.0.0 整個子網路，可執行 KB824146Scan.exe 192.168.0.0/24。

3. 解決方法

請安裝微軟所提供 MS03-039 修補程式

http://www.microsoft.com/taiwan/security/bulletins/MS03-039.asp

建議於防火牆擋掉外部網路對內部 TCP/UDP Port 135 的存取，亦建議擋掉 UDP Port 137/138/445 與 TCP Port 139/445/593。

4. 參考資訊

http://www.microsoft.com/taiwan/security/bulletins/MS03-039.asp

http://www.cert.org/advisories/CA-2003-23.html

二、Cisco IOS DoS 弱點

1. 簡要說明

IOS (Internet Operating System) 為 Cisco 網路設備(路由器，交換器…)所使用的作業系統，其被發現含有阻斷服務的弱點。攻擊者可以透過傳送特殊的封包，造成 Cisco 網路設備無法正常運作，幾乎所有支援 IPv4 的

Cisco 網路設備均受此弱點影響。

2. 檢測方法

可於登入 Cisco 網路相關設備後，執行 show version 查看 IOS 的版本，比較 http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml 所列版本以決定是否有此弱點。如果於 92 年 7 月之後未做過 IOS 更新者，幾乎都含有此弱點。

3. 解決方法

最好能升級 IOS 至最新版本，但因升級 IOS 所需技術能力較高，且通常需與 Cisco 簽有契約，建議未升級過 IOS 者尋求廠商協助。

對於無法升級 IOS 者，可先設定 ACL 防止遭受阻斷服務攻擊。下列的 Access List 是特別針對阻擋攻擊的封包而設計的。請注意攻擊的封包可能來自於假冒的來源位址，所以請把此 Access List 套用至所有路由器的介面上，且同時套用於進入及送出雙向交通。如果有的話，也請繼續使用你原來有的 Access List，最好將兩個 List 合而為一。

```
access-list 101 permit tcp any any
access-list 101 permit udp any any
access-list 101 deny 53 any any
access-list 101 deny 55 any any
access-list 101 deny 77 any any
access-list 101 deny 103 any any
!--- 請將你原有的 Access List 插入此處
!--- 你如果有用任何其他路由協定，也請你 permit
!--- 它的交通，所以以前的 Access List 會正常運作；
!--- 或是你可以使用 permit ip any any (如下) 讓所有協定都可運作
access-list 101 permit ip any any
```

如果你有使用 PIM (如果一個介面有使用 PIM，介面上的設定會有 ip pim dense-mode, ip pim sparse-mode, 或 ip pim sparse-dense-mode 指令存在)，那您將不需要加入 access-list 101 deny 103 any any 這一行。

要把 Access List 套用至介面上，請使用下列指令：

```
(config-if)# ip access-group 101 in
(config-if)# ip access-group 101 out
```

4. 參考資訊

請參考下列網址

http://www.cert.org/advisories/CA-2003-17.html

http://www.cert.org/advisories/CA-2003-15.html

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

三、SNMP 預設 Community Name

1. 簡要說明

SNMP (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。其使用 Community Strings 為其認證機制，通常又分為唯讀與可寫入兩種權限，各設備通常會有預設的 Community Strings，如以 public 當成唯讀的 Community String，以 private 當成可寫入的 Community String。攻擊者如果知道唯讀的 Community String，則可藉此獲取所需資訊；攻擊者如果知道可寫入的 Community String，則可藉此竄改網路設備的設定。此外約於 91 年 2 月左右，多個 SNMP 的實做亦被發現含有 DoS 弱點。

2. 檢測方法

技服中心將利用 Nessus，使用幾組常用的 Community Strings 作測試，檢測是否可透過 SNMP 存取網路設備。

3. 解決方法

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。

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

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。

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. 參考資訊

請參考下列網址

http://www.sans.org/top20/#w10

http://www.sans.org/top20/#u7

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

四、Messenger 服務緩衝區溢位弱點(MS 03-043)

1. 簡要說明

Messenger service 為 windows 類型主機的一個 service，使用者可以經由此 service，使用"net send"指令傳送訊息給其他的 windows 主機，以達到傳送訊息的用途，通常是管理者用來廣播訊息給其他使用者。而此服務被發現存在有緩衝區溢位弱點，原因在於此服務並未檢查傳送的資料長度，就將其送至分配的記憶體位置，結果造成攻擊者可能經由此弱點，藉由傳送特殊的 message 資訊給有弱點的主機，將得以系統上 Local System 的權限執行任意程式。

值得注意的是，messenger service 與 Microsoft Messenger 或 MSN Messenger 是不同的，messenger service 僅能傳送純文字的訊息，並且是系統安裝時便已存在，後兩者則可用來傳送文字、影像和圖片等等資料，並且需要額外安裝。

2. 檢測方法

技服中心將使用弱點軟體進行掃描，並偵測是否有此弱點存在，而在本機上想知道是否有存在弱點，首先從系統上的服務，確定 messenger service 是否啟動，若無啟動則無此弱點。接著從 Register Key 登錄值檢查是否已安裝修補程式，依據不同的系統，分別如下：

(1) NT 4：

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\KB828035

(2) Windows 2000：

HKLM\SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB828035

(3) Windows XP：

HKLM\SOFTWARE\Microsoft\Updates\Windows XP\SP2\KB828035

(4) Windows 2003：

HKLM\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP1\KB828035

若有以上的 register key 值存在，則代表系統上已安裝此修補程式，無此弱

點，反之，則代表系統上存在弱點。

註：上述的 register key 僅代表目前的情況，未來各系統若有推出新的 service pack，後續的 service pack 將包含此修補程式，則上述的值很可能有所改變，還請留意，例如，windows 2000 的 service pack 5 出現時，則 HKLM\SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB828035 可能因此而被取代。

3. 解決方法

(1) 若不需要 messenger service 的話，可考慮關閉此 service，方式為

(a) 點選"開始"，選擇"控制台"(或點選"設定"，再選擇"控制台")。

(b) 點選"系統管理工具"。

(c) 點選"服務"。

(d) 點選"Messenger"。

(e) 在其中的啟動類型中，選擇停用。

(f) 點選"停止"，並點選"確定"。

(2) 安裝修補程式，不論是否要停用 messenger service，皆應安裝修補程式，修補程式的安裝方式可採用 Windows Update(建議採用此方式，因為較為簡單，而且同時安裝多個修補程式亦很方便，可從 windows 的"開始"中選擇)。或是直接下載此修補程式(MS 03-043)，網址為：http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-043.asp，從中選擇所用的作業系統版本。並下載修補程式後安裝。安裝修補程式後，再自行由 register key 檢查修補程式是否安裝成功。

4. 參考資訊

http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-043.asp

http://www.kb.cert.org/vuls/id/575892

五、Sendmail Prescan Function 緩衝區溢位弱點(CA-2003-25)

1. 簡要說明

Sendmail 為著名的 MTA(Mail Transport Agent，即為郵件轉送程式)軟體，為目前佔有率最高的 MTA 軟體，而在今年 9 月中出現一個新的緩衝區溢位，原因在於其中的 prescan()函數對於攻擊者送來的特殊郵件內容處理不當，結果使得攻擊者得以 sendmail daemon(即 windows 系統上的 service，在 unix 系統上稱為 daemon)的權限執行系統上的任意程式，而此權限有可能是 root 權限。此弱點存在於 sendmail 8.12.10 版之前(包含 5.79 到 8.12.9)，另外商業版的 sendmail 軟體同樣有此弱點，包含有 Sendmail Switch, Sendmail Advanced Message Server (SAMS), and Sendmail for NT。

由於此弱點是經由特殊內容的郵件內容來攻擊，而非較低層的網路封包，因此未含有此弱點的 sendmail 程式或是其他的 MTA 軟體(如 Exchange)，依然會轉寄有問題的郵件給其他的 sendmail，結果將造成更大的危害。

2. 檢測方法

(1) Solaris

Solaris 7、8、9 皆有此弱點存在，檢測的方式可以經由/usr/bin/mconnect 指令，觀察回應訊息，對於 Solaris 7 與 8 而言，若出現的資訊為 8.11.7+Sun 代表系統上的 sendmail 存在有弱點，若是回應的資訊為 8.11.7p1+Sun，代表系統已安裝修補程式，若對於 Solaris 9 而言，回應的資訊若為 8.12.9+Sun，代表系統上的 sendmail 存在有弱點，8.12.10+Sun 代表系統已安裝修補程式。

(2) RedHat Linux

目前仍有支援的 RedHat Linux 系統版本為 7.1、7.2、7.3、8.0 與 9 版(較舊的版本已不再支援，請更新到上述的版本)，對於上述版本是否有安裝此弱點的修補程式，請執行 rpm –q sendmail 指令，若出現的資訊為：

(a) 7.1 版

sendmail-8.11.6-27.71

(b) 7.2 版

sendmail-8.11.6-27.72

(c) 7.3 版

sendmail-8.11.6-27.73

(d) 8.0 版

sendmail-8.12.8-9.80

(e) 9 版

sendmail-8.12.8-9.90

(詳細資訊，參考 https://rhn.redhat.com/errata/RHSA-2003-283.html)，則代表系統上的 sendmail 是無此弱點的，若是出現的值中的 release 號碼(如上述中的 sendmail-8.11.6-x.ZZ 與 sendmail-8.12.8-y.ZZ 中的 x 與 y 數字，如此處的 x=27, y=9)是比本文所列的還少的話，代表系統存在此弱點，若相等的話，代表系統已安裝此最新修補程式，若出現的數字較大的話，則代表系統上安裝了比此弱點更新的修補程式(此情況將出現在未來有出現同樣為 sendmail 弱點的情形下，且安裝了新修補程式，故在目前是不可能發生的)。

(3) FreeBSD

目前仍有支援的版本為 4.7、4.8、5.0 與 5.1 版，4-stable 版，對於較舊的版本，建議更新至上述版本，更新的方式請參考 http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/cutting-edge.html

至於上述的版本，欲檢查是否存在有弱點，請使用

pkg_info | grep sendmail

若是有出現 sendmail 的資訊，且高於或等於 8.12.10 者，代表系統上的 sendmail 是無弱點的，若低於此版，則代表有弱點，而若上述的結果並未發現有 sendmail 的資訊，則檢查檔案：/usr/libexec/sendmail/sendmail 的日期，若是該檔的日期是比 2003 年 9 月 17 日還新的檔案，代表系統無此弱點，反之則系統存在此弱點。

3. 解決方法

(1) Solaris

參考網站：http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/56860 所列的修補方式，在其中選擇所用的硬體架構(如 SPARC 或 x386)與版本，連結至新網頁後，下載修補程式後，使用 patchadd 指令安裝修補程式，方式為 patchadd < /var/spool/patch/patch_file，其中/var/spool/patch 代表放置修補程式的目錄，patch_file 代表修補程式檔名，如 110615。

註：由於系統安裝上的程式具有相依性，因此在安裝上述的修補程式時，須注意是否有安裝該修補程式的相依修補程式(在各個修補程式網頁中，皆會說明所需要的修補程式為何)，因此，若是對於有許多的弱點皆需修補的系統而言，建議採用一次同時安裝多個修補程式的方式進行，此方式為安裝 Solaris 的 Recommend.zip 修補程式，Recommend.zip 包含有該系統中所有(含最新)的修補程式，網址為：http://sunsolve.sun.com/pub-cgi/show.pl ，使用方式請參考該網站的說明。

(2) RedHat Linux

請至 https://rhn.redhat.com/errata/RHSA-2003-283.html 網站上下載 sendmail 的修補程式，如以一般常見的 x386 電腦架構而言，請將個別版本中屬於 i386 的四個檔案下載至本機上(建議建一目錄專門放置新的 rpm 檔，如建立/var/rpm 目錄)，下載後進入此目錄，執行

rpm –Fvh *.rpm

如此將安裝關於 sendmail 的修補程式於系統上，而上述的方式為安裝個別套件的修補程式的方式，若是要對整個系統上的弱點進行修補的話，建議使用 up2date 工具，詳細使用方式請參考相關說明文件，或是參考技服中心網站(http://www.icst.org.tw)上的 RedHat linux 的修補程式安裝說明。

(3) FreeBSD

系統上的 sendmail daemon，可能是經由系統設定而啟動(安裝系統時皆已含有 sendmail 的程式，只是不一定有設定為啟動)，或是經由 ports 安裝的(位置在/usr/port/mail/sendmail)。

(a) Sendmail 為隨系統一併安裝的情況

系統上需要有系統的 source code 才可進行修補，同樣地，若是僅

安裝單一修補程式的情況，可直接使用 patch 指令，方式為下載修補程式後，執行以下：

```
# cd /usr/src
# patch < /path/to/patch
# cd /usr/src/lib/libsm
# make obj && make depend && make
# cd /usr/src/lib/libsmutil
# make obj && make depend && make
# cd /usr/src/usr.sbin/sendmail
# make obj && make depend && make && make install
```

詳細說明，參考

ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:13.sendmail.asc

(b) Sendmail 為由 ports 額外安裝的情況

請使用 cvsup 工具更新 ports 裡的檔案，關於使用 cvsup 工具的方式，參考

http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/cvsup.html

接著移除舊版的 sendmail 程式(使用 pkg_delete filename 方式移除，filename 可用 pkg_info 指令得到)，並在/usr/ports/mail/sendmail 目錄下，執行 make install 安裝新版的 sendmail 程式。

註：上述的兩個方式為安裝此單一修補程式的情形，若是一次同時安裝許多修補程式，可使用 cvsup 工具將系統的 source codes 更新後，再使用"make world"指令一次更新整個系統。參考前述更新方式的網址：

http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/cutting-edge.html

(4) 商業版的 sendmail

請聯絡購買此產品的廠商，獲得修補程式的支援。

4. 參考資訊

http://www.cert.org/advisories/CA-2003-25.html

http://www.securityfocus.com/archive/1/337839

六、網站主機權限管制不當 - 危險的 HTTP PUT method

1. 簡要說明

HTTP (HyperText Transfer Protocol - 超本文傳輸協定) 是目前網頁伺服器所使用的傳輸協定，其提供一種 PUT method 以讓 Client 端可以上傳檔案至 Server 端。在大部分的網頁伺服器預設組態下，PUT method 應該是無法隨意使用，因為啟動 PUT method 將使攻擊者可任意上傳檔案至 Server

端，達到其置換網頁的目的，若攻擊者上傳惡意程式至有執行權限的目錄，將可達到更大的破壞。若網站主機權限管制不當，將造成任一使用者均可使用 HTTP PUT。最近發現部分單位遭利用 HTTP PUT 置換網頁，請對所屬網頁伺服器進行檢查，以防網站遭駭。

2. 檢測方法

技服中心將嚐試以 HTTP PUT 對網站寫入檔案，以判定是否有此問題。

3. 解決方法

微軟 IIS 系統請完成以下三個步驟以預防不預期的 HTTP PUT：

i. 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。

ii. 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。

iii. 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