一、DNS 伺服器—Bind overflow 弱點

1. 簡要說明

DNS(Domain Name System)服務，用途在於將主機名稱(Host Name)轉成 ip 位址，例如將 www.example.com 轉成某一 ip 位址，好處在於對於人類而言，不需記憶眾多難記的數字，而可以較熟悉的名稱與網路伺服器進行溝通。而 DNS 的主要目的即為此，當然除了上述的主機名稱轉 ip 外，ip 轉主機名稱的功能也是存在的。因此，DNS 服務可說是目前網路服務的基礎，若無 DNS 服務，則郵件的傳送與網站的連結等，都將受到重大影響，因為許多網路服務皆需要 DNS 服務作轉址(主機名稱與 ip 位址的轉換)的支援。在 DNS 程式中，以 Bind (Berkley Internet Name Domain)最著名，也最引起駭客的興趣，而 Bind 出現的問題中，除了設定上的錯誤或遭受 DoS 攻擊情況外，最嚴重的問題在於 Bind 程式本身的問題，例如存在有緩衝區溢位(buffer overflow)弱點，而此類的弱點，往往會讓攻擊者得以系統上執行 Bind 程式的權限(有可能是 root 權限，尤其是較舊的 Unix 系統)，執行系統上的任意程式，造成重大的危害，且 Bind 程式至今已出現過多次的緩衝區溢位問題，因此，不可不重視此弱點所造成的後果。

2. 檢測方法

可使用 dig 工具測試目前所使用的 Bind 版本為何，方式為

dig @target version.bind chaos txt

其中的 target 用 ip 代替，例如 192.168.0.1。或是在本機上使用 named –v，系統將回應 Bind 的版本訊息。

若對 RedHat 系統而言，若是系統的版本是 7.3 以前(含 7.3)，代表系統上的 Bind 可能存在問題，需要進一步檢查，檢查的方式如下：

rpm –q rpm_package_filename (將 rpm_package_filename 改成以下表格的 RPM name)

System Version	RPM name	Correct version
7.0	bind	bind-9.2.1-0.70.2
	nscd	nscd-2.2.4-18.7.0.4
7.1	bind	bind-9.2.1-0.71.1
	nscd	nscd-2.2.4-27
7.2	bind	bind-9.2.1-1.7x.2
	nscd	nscd-2.2.4-27
7.3	bind	bind-9.2.1-1.7x.2
	nscd	nscd-2.2.5-37

若是系統回應的 version 跟上述的表格相同或較新的話，代表系統上並未存在弱點，若是較舊的話，代表系統上存在弱點。

至於其他的平台，請參考以下兩個網址的說明判斷有無弱點：

http://www.cert.org/advisories/CA-2002-19.html
http://www.cert.org/advisories/CA-2002-31.html

3. 解決方法

建議安裝新版的 Bind，關於最新的版本的資訊，請參考 Bind 的網站，網址為：http://www.isc.org/products/BIND/，若是隨各作業系統(如 Solaris、RedHat Linux 等)安裝的 Bind 程式，通常各作業系統的維護廠商或團體會自行提出解決方法，例如推出修補程式、更換新版 Bind 等等。關於各系統的修補方式，請參考各相關網站的說明(以下的方式不僅修補 Bind 的弱點，更將修補系統上的所有問題)，條列如下：

(1) Sun Solaris

請至 Sun 網站下載修補程式(若是想安裝全部的修補程式，請安裝 Recommend.zip 修補程式)，網址為：http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage。

(2) RedHat Linux

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

請至 http://www.freebsd.org/security/網站安裝相關的修補程式，或是使用 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。參考以下網址：
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/cutting-edge.html

4. 參考資訊

http://www.cert.org/archive/pdf/dns.pdf
http://www.cert.org/advisories/CA-2002-31.html
http://www.sans.org/rr/catindex.php?cat_id=17

二、FrontPage Server Extension(FPSE) overflow 弱點(MS 03-051)

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。而在本季的掃描中，所掃描的部分是於 2003 年 11 月出現的新弱點，此弱點在於 FPSE 處理 chunked 的資訊時，並未檢驗其輸入的長度，結果會出現 buffer overflow 的情況，導致攻擊者可執行系統上的任意指令，或是造成有 FPSE 支援的網站暫時無回應，而無法提供服務。

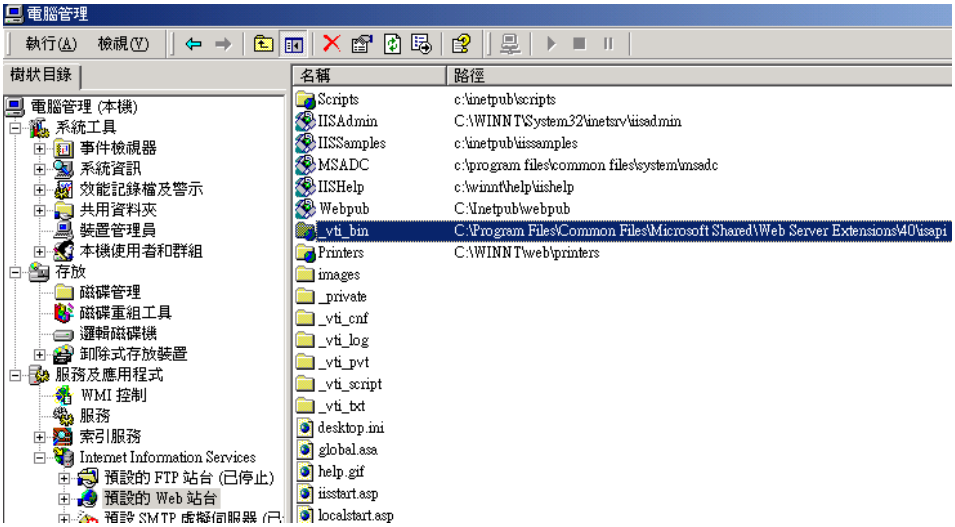
2. 檢測方法

由於系統在安裝修補程式前後的情況會有所不同，所以技服中心將嘗試對 web 網站送出 chunked 方式的 request，藉由觀察回應的資訊來判斷有無弱點，至於直接由系統上檢查的方式如下：

(1) 判斷系統上所用的 FrontPage Server Extension 版本

首先判斷系統上所安裝的 FPSE 的版本為 2000 或是 2002，而由於系統上的 FPSE 可能由多種方式安裝至系統上。如隨著 windows 系統光碟一併安裝或隨著 Office 安裝時一併安裝的。所以需先檢查系統上的 FPSE 為何。因為不同的 FPSE，需要檢查的檔案也會不同。而安裝修補程式後的情況也會不同。

另外亦可從 IIS 的管理介面中檢查所用的 FPSE 為幾版，例如以下的例子顯示的是 FPSE 2000 的情況。因為其中的_vti_bin 虛擬目錄所指的路徑為 C:\Program Files\Common Files\Microsoft Shared\web server extensions\40，而其中的 40 代表 FPSE 2000。若是此目錄出現的是 50 的話，代表系統上所安裝的是 FPSE 2002。



(2) 對於 FPSE 2000 的檢查

請檢查以下檔案的版本：

請確認所檢查的檔案是位於以下目錄或其下的子目錄：

C:\Program Files\Common Files\Microsoft Shared\web server extensions\40

因為以下需檢查的檔案可能同時有好幾個，所以需留意是否位於以上目錄。其中上述目錄中的 40 代表的是 FPSE 2000，

檔案名稱	版本
fp4awel.dll	4.0.2.7802
fp30reg.dll	4.0.2.7523
fpsrvadm.exe	4.0.2.7523

若是系統上的版本與上述相同者，代表已安裝修補程式，若所查出

的版本資訊低於上述版本者，代表尚未安裝修補程式。

另外系統上不一定會存在 fp30reg.dll 檔案，若為此情形，可略過此檔案的檢查。

(3) 對於 FPSE 2002 的檢查

請檢查以下檔案的版本，同樣請確認以下目錄位於 C:\Program Files\Common Files\Microsoft Shared\web server extensions\50 下

檔案名稱	版本
fp5awel.dll	10.00.4803.0000
fp30reg.dll	10.00.4205.0000
fp5Areg.dll	10.00.4205.0000

若是系統上的版本與上述相同者，代表已安裝修補程式，若所查出的版本資訊低於上述版本者，代表尚未安裝修補程式。另外系統上不一定會存在 fp30reg.dll 檔案，若為此情形，可略過此檔案的檢查。

3. 解決方法

(1) 若不需要 FPSE，請考慮移除，移除方式請參考本中心之前定期掃描所列的說明文件。

(2) 若需要 FPSE 支援，請務必安裝修補程式：

參考以下網址的說明，安裝修補程式，網址為：

http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-051.asp

其中請依據系統上所安裝的 FPSE 的方式來安裝修補程式，例如若是系統上的 FPSE 是隨 windows 系統一併安裝的話，使用 windows update 即可安裝修補程式，若是由安裝 Office 套件後一併安裝的，請下載對應的修補程式，安裝修補程式。

4. 參考資訊

http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-051.asp

三、Cisco 路由器 Web 管理介面未正確設定安全存取權限

1. 簡要說明

Cisco 路由器提供多種管理方式，如透過 Console 線、使用 Telnet 及透過 Web 介面等。若路由器管理者開啟 Web 管理介面，卻未正確設定安全存取權限，則任何人只要知道該路由器的 IP，均可使用瀏覽器變更該路由器設定，造成網路連線上的問題。

2. 檢測方法

直接使用瀏覽器連接該路由器，若可不經身分驗證便完成更改設定動作，便是未正確設定安全存取權限。

3. 解決方法

如果不需要用到 Cisco Web browser UI 的話，請直接下此一指令(執行下述的各指令前，請先進入 global mode 中)：

no ip http server

如果一定要使用 Cisco Web browser UI 的話，請設定存取的權限：
可以先設定 ip http access-class 只允許特定的 IP 進行存取。以下是個例子：

ip http access-class icst
ip access-list standard icst
permit 192.168.34.0 0.0.0.255
permit 172.16.0.0 0.0.255.255
permit 10.0.0.0 0.255.255.255

這個例子是建立一個名叫 icst 的 standard access-list，只允許 192.168.34.0/24，172.16.0.0/16，以及 10.0.0.0/8 三個網段對 Cisco Web browser UI 進行存取，其他所有 IP 及網段皆被禁止存取。

接下來可以在路由器上設定使用者帳號及密碼，更仔細的過濾存取的使用者：

aaa new-model
aaa authentication login default local
aaa authorization exec default local
username icst privilege 15 password 1234
username bob privilege 1 password 5678
ip http server
ip http authentication local (如果是 IOS 11.2 或之前的版本，用 **aaa** 取代 **local**，其他版本均可用 **local**)

如以上例子，使用者 icst 可以下所有的指令 (enable mode)，而使用者 bob 只能使用一般指令 (normal)。您可以視需要將使用者訂定不同的 privilege levels。

備註：請記得於設定後於"Privileged Mode"中執行
cp running-config startup-config
將目前的設定檔儲存至 Nvram，以防重開機後以上設定消失。

參考資訊

Cisco HTTP Server 的設定可參考

http://www.cisco.com/warp/public/480/http-1.pdf