92 年第二季 偵測弱點之說明修補方式

一、IIS 5.0 WebDAV overflow 弱點(MS 03-007)

1. 簡要說明

WebDAV 為 World Wide Web Distributed Authoring and Versioning 的簡稱，作為 HTTP 協定的延伸。WebDAV 協定作為 web 介面的編輯與檔案管理用途，在 windows 2000 上首次採用此協定。而問題出現在處理 WebDAV request 的 Ntdll.dll 對於傳來的 request 並未正確驗證，而導致緩衝區溢位以致於導致攻擊者得以利用系統上執行 IIS service 的權限(通常是系統上的 LocalSystem 權限)執行系統上的任意程式。風險程度相當高。
微軟對此弱點的編號為 MS 03-007
註：此問題出現在 windows 2000 主機上。

2. 檢測方法

對於不清楚系統上是否已經安裝此修補程式，請於安裝 IIS 5.0 的主機中，檢查以下的 register key 是否存在(請在開始程式中選擇執行，並輸入 regedit 開始登錄編輯程式)。
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP4\Q815021
若存在代表系統上已安裝此修補程式—MS 03-007，若不存在則代表系統尚未安裝修補程式，並極可能存在弱點。

3. 解決方法

建議安裝修補程式，網址為
http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&displaylang=en
選擇所用的 OS 語系下載修補程式，另外此修補程式雖然可同時用在 windows 2000 SP2 或 windows 2000 SP3 已安裝的系統上，不過對於 windows 2000 SP2 的系統，可能發生安裝修補程式後系統無法運作的錯誤情況，若系統上的 ntoskrnl.exe 是在 5.0.2195.4797 到 5.0.2195.4928 之間的版本會出現此不相容的問題，這個問題可以經由先安裝 windows 2000 SP3 再安裝修補程式的方式來克服。因此若系統尚未安裝 windows 2000 SP3，請先安裝，windows 2000 SP3 下載網址為：
http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/default.asp

4. 參考資料：

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

-007.asp
http://support.microsoft.com/default.aspx?scid=kb;en-us;815021
http://www.securityfocus.com/bid/7116

二、IIS 4.0 Sample file 弱點

1. 簡要說明

IIS 4.0 安裝過程中可能一並安裝了 ExAir 此範例站台，在 ExAir 中的 advsearch.asp、search.asp 及 query.asp 存在有 DoS 的弱點，攻擊者可藉由此弱點導致系統上的 CPU 使用率達到 100%，以致無法進行正常的運作。
註：此範例程式弱點存在於 NT 4.0 的主機上。另外還有一些如 showcode.asp、codebrws.asp 等等範例程式則有洩漏系統上資訊的問題存在。

2. 檢測方法

可使用 web browser 連線至受測主機上，並且使用以下 request 來判斷。
http://hostname/iisamples/exair/search/advsearch.asp
http://hostname/iisamples/exair/search/search.asp
http://hostname/iisamples/exair/search/query.asp
http://hostname/msadc/Samples/SELECTOR/showcode.asp
http://hostname/iisamples/exair/howitworks/codebrws.asp
若回應的是 404 Not found 的錯誤訊息，則代表系統上應不存在上述 asp 程式，另外亦可使用系統上的搜尋工具檢查上述 ASP 程式是否存在(需注意的是，若是系統上有自行開發的 ASP 程式，有可能所使用的檔名剛好相同，此時請注意不要弄錯檔案)，

3. 解決方法

對於提供服務的主機，建議不要安裝範例程式，若已經安裝了範例程式，建議將整個範例程式所目錄移除(在該目錄中的程式皆是系統安裝，而非自行開發的前提下)，或是將上述的 ASP 程式移除。

4. 參考資訊

http://www.securityfocus.com/bid/167
http://www.securityfocus.com/bid/193

三、DNS zone transfer

1. 簡要說明

DNS server 上註冊的資訊，含有單位內的 hostname 與 ip 的對應資訊，對

於洩漏這些資訊可能導致攻擊者可以進一步判斷攻擊的目標，攻擊者藉由 DNS zone transfer 的 request 可以獲得此 DNS server 上註冊的資訊(其中亦可能含有主機名稱的內部對應 ip 資訊)，如此有助於攻擊者更了解所屬網域的架構及擬定攻擊策略。

2. 偵測方法

Windows 主機可使用 nslookup 工具測試(請使用非受測 DNS server 以外的電腦，進行測試)，方式如下

(1) 在開始→執行中輸入 cmd，啟動 dos 模式。

(2) 輸入 nslookup

(3) 指定欲測試之 DNS 主機的 ip，並送出 DNS zone transfer 要求

> server [my_dns_ip]

> set type=any

> ls –d [my_domain]

其中[my_dns_ip]請改成該 DNS server 的 ip，如 163.163.163.3，而[my_domain]請改成該 DNS server 管理的 Domain，如 example.gov.tw。

(4) 若是出現錯誤訊息，代表系統無此問題，若是列出資訊，則代表系統有 Zone transfer 的問題。

Unix like 主機的測試方式亦可使用 nslookup 指令，或是使用以下方式測試。

host –l –v –t any [my_domain]

3. 解決方式

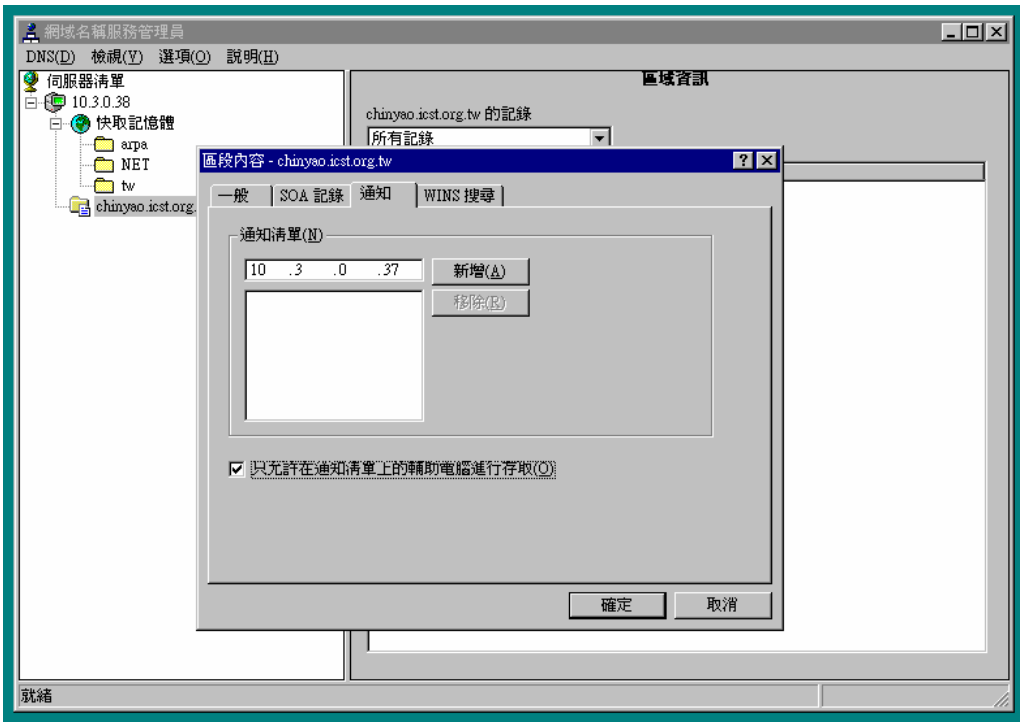
Windows 主機

限制可執行 DNS zone transfer 的對象，方式如下

設定僅允許 Zone transfer 至特定主機說明

(1) 在網域名稱服務管理員選擇所管理之網域名稱，按滑鼠右鍵選內容。

(2) **在其中的通知中，新增一筆另一台** DNS server **的** ip(**作為** secondary DNS server)，**點選新增，並勾選只允許在通知清單上的輔助電腦進行存取，再點選確定即可。若不需要** secondary DNS server **的話，則僅勾選只允許在通知清單上的輔助電腦進行存取即可。**



Unix Bind

請在原先的 named.conf (**通常位於**/etc/named/**下)中加入以下設定**

假設原先的設定為：

```
options {
        directory       “/var/named”;
        forwarders      {x.x.x.x;};
};
```

變更為

```
options {
        directory       “/var/named”;
        forwarders      {x.x.x.x;};
        allow-transfer  {x.y.z.t ;};
};
```

注意僅需更改紅字部分。其中 x.y.z.t **請換成需要執行** zone transfer **的主機或網段，並重新啟動** name server**，詳細說明，請參考所用** Bind **的說明。**

4. **參考資訊**

   http://www.sans.org/rr/firewall/DNS_sec.php

四、Telnet server

1. **簡要說明**

   Telnet server **為** Unix like **主機或是** router**、** switch **中常見的遠端管理工具，這個** service **的弱點在於所傳送的資訊是屬於未加密的，因此會出現封包竊聽攻擊問題。當攻擊者竊取到帳號擊密碼之資訊後，將可利用此登入系統，針對系統進行破壞，因此建議設定使用限制或是以其他** service **代替，例如使用** SSH **代替。**

2. **偵測方法**

   可直接嘗試在 Windows **的** dos **模式中輸入**

   telnet target_ip

   或在 Unix like **主機的** terminal **中輸入**

   # telnet target_ip

   若有出現登入帳號提示畫面，則是系統上有 telnet server**，若無法連線或是錯誤訊息則代表受測** ip **並無** telnet server**。**

3. **解決方法**

   Unix like **主機**

   通常 telnet server **的啟動的設定是在**/etc/inetd.conf **中，若不需要** telnet**，在** telnet **開頭的那行文字前加入**#**符號，並重新啟動** service **或重新開機即可，方式為：**

kill –HUP `sed q /var/run/inetd.pid`

若是 RedHat linux 的話，可執行 ntsysv 指令，並將 telnet server 前的＊符號取消，之後再重新啟動 xinetd service，方法如下

service xientd restart

若是需要類似 telnet 之類的遠端管理工具，建議使用 SSH，若是 linux 系統一般在系統安裝時便已經安裝了 SSH server，可直接使用，若是 Solaris 或 AIX 的主機則需要自行安裝，關於 Solaris，可參考以下網址：

http://www.unixguide.net/sun/ssh_installation.shtml

或是 Openssh 的網站：http://www.openssh.org

另外 openssh 亦可能出現弱點，因此仍需留意是否有關於 openssh 的弱點出現，適時安裝修補程式。

以上為移除 telnet server 並以 ssh 取代的方式，若是需要 telnet server，則建議以防火牆或 router 的 ACL(access control list)，限制連線來源。

Cisco router 設定建議

若存在 telnet server 的 ip 是屬於 router 的話，建議取消 telnet 的遠端管理，僅使用 console 的方式管理，若需要 telnet 管理的話，則建議設定可以使用 telnet 管理工具的來源，方式如下：

首先 create 一個 access-list:

Router(config)# access-list 10 permit 10.3.0.40 0.0.0.0 (如果不是單一主機，例如 10.3.0.0/24 整個網段，輸入 10.3.0.0 0.0.0.255)

Router(config)# access-list 10 deny any

然後 apply 此 list 到 VTY line:

Router(config)# line vty 0 4 (請自行檢視您的 Router 有多少 line vty，然後 apply to all of them)

Router(config)# access-class 10 in

這樣就行了

若是其他的 network device，請參考其使用手冊加以設定。