95 年第二季定期弱點掃瞄之說明與修補方式

一、 網站用戶端服務(Web Client Service)可被遠端執行程式碼弱點(MS 06-008)

(一) 簡要說明：

Web Client Service(WebClnt.dll)為微軟作業系統中，用來存取 Internet 上文件的服務，其允許 W32 的應用程式藉由 WebDAV 協定的規範，得以創造、讀寫檔案。而 WebDAV 為利用 HTTP 協定進行主機間檔案存取之協定。本弱點產生之原因在於 Web Client Service 未對使用者輸入資料之長度進行驗證，以致出現緩衝區溢位的弱點，結果使得攻擊者經由特殊內容之輸入資料，得以對系統進行惡意之程式安裝，讀取、變更或是刪除系統上檔案，或者新增系統上具完整權限之帳號。而為了利用此弱點，攻擊者需先擁有系統登入之資訊，因為對於匿名之使用者而言，無法經由此弱點進行攻擊。然而若是系統上的 Guest 帳號被啟動的話，則此項弱點可被任何使用者利用。

本弱點存在於 Windows XP 與 Windows 2003 系統上，本項弱點存在於當 Web Client 服務為啟動之情況。在 Windows 2003 上，此服務預設為關閉的，而 Windows XP 則有可能為啟動之情況。

(二) 檢測方法

1. 使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 20928 進行偵測，依此判斷是否存在弱點。

2. 使用微軟工具檢查

使用微軟的 MBSA 工具檢查此修補程式是否已安裝，或者使用 Windows Update 工具直接向微軟網站檢查是否已安裝此修補程式。

(三) 修補方式

下載 MS06-008 的修補程式，網址為：

http://www.microsoft.com/taiwan/security/bulletin/MS06-008.mspx

或者使用 Windows Update 服務進行修補，若為多台主機情況，亦可使用 SUS，網址為：

http://www.microsoft.com/windowsserversystem/updateservices/evaluation/previous/default.mspx

、WSUS，網址為：

http://www.microsoft.com/taiwan/windowsserversystem/updateservices/evaluation/overview.mspx

或 SMS，網址為：

http://www.microsoft.com/taiwan/smserver/evaluation/capabilities/patch.htm

進行修補。另在安裝修補程式之外，建議使用防火牆阻擋來自 Internet 對內部系統(含內部網路或是 DMZ 區的系統)之 TCP port 139 與 445 的存取，以增強對 Windows 系統之防護。

(四) 參考資料

微軟官方說明文件：

http://www.microsoft.com/taiwan/security/bulletin/MS06-008.mspx

其他相關說明文件：

http://www.kb.cert.org/vuls/id/388900

http://www.ciac.org/ciac/bulletins/p-224.shtml

二、 HTTP dangerous method (PUT, Delete)弱點

(一) 簡要說明

HTTP dangerous method 弱點在於 HTTP 提供經由 HTTP 協定的方式，可以針對 Web server 進行檔案上傳與刪除，如此若是 Web server 權限設定不當時，將可能發生網頁出現不預期的修改情況，一般而言預設之權限應無包含刪除與上傳，但仍有可能出現不慎開啟的情況。本弱點並非軟體設計錯誤類型，故無法經由安裝修補程式補強。本弱點為系統設定不安全而產生的，並且攻擊者可經由此情況進行網頁之變更與刪除。因此雖然先前已針對此項弱點進行偵測，然而此項弱點仍不斷出現，因此於本季中再次進行偵測。

(二) 檢測方式

1.使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 10498 進行偵測，依此判斷是否存在此弱點。

2.使用 Telnet 工具檢查

使用 Telnet 工具與受測網站建立連線後(如 telnet web_ip 80)，輸入以下兩行指令檢查，

OPTIONS / HTTP/1.1

Host:example.com

若於回應訊息裡的"Allow："該行發現 DELETE 或 PUT 的話，則代表系統存在弱點，應該進行修正。範例如下：

```
telnet [redacted] 80
OPTIONS / HTTP/1.1
Host: example.com

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Fri, 31 Mar 2006 06:53:34 GMT
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE
D, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND,
```

(三) 修補方式

1.針對微軟 IIS 伺服器的修補方式，請完成以下三個步驟以預防此問題：

(1) 如果該網站不需使用 WebDAV (Web Distributed Authoring and Versioning)，建議將其關閉。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。

(2) 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。

(3) 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。

2.針對 Apache 伺服器的修補方式，請在欲保護之網頁目錄上加上<Limit>以及<Limit Except>設定值，例如：

```
<Limit GET HEAD POST OPTIONS>
    Order allow,deny
    Allow from all
</Limit>
<LimitExcept GET HEAD POST OPTIONS>
    Order deny,allow
    Deny from all
</LimitExcept>
```

代表僅允許 GET, HEAD, POST, OPTIONS 等 HTTP 1.1 method，其他不允許。設定完後重新啟動 Apache 套用新值。有關詳細設定方式，請參考：http://wiki.linuxquestions.org/wiki/Securing_Apache#Disabling_PUT_and_DELETE

(四) 參考資料

http://wiki.linuxquestions.org/wiki/Securing_Apache
http://www.securityfocus.com/bid/12141

三、 Windows Plug and Play 服務可讓攻擊者執行系統程式弱點(MS 05-039)

(一) 簡要說明：

Windows 使用 Plug and Play 服務用來偵測系統安裝的硬體，譬如於 Windows 系統上接上滑鼠時，系統將偵測該滑鼠，載入必要的驅動程式以讓使用者使用。本項服務於 2005 年 8 月遭發現存在緩衝區溢位的弱點，結果導致遠端攻擊者可經由傳送特定格式之封包給 TCP port 445，讓攻擊者取得系統上的完整權限，或者產生阻斷服務(DoS)攻擊之情況，另已發現有自動化的電腦蠕蟲(例如 Zotob worm)針對此弱點進行感染攻擊，實為嚴重之問題，此外本機上的非管理者權限使用者亦可能經由此弱點取得管理者之權限。受本項弱點影響之平台包含 Windows 2000, Windows XP 與 Windows 2003，而 Win 98 與 Win ME 並無此弱點，至於 Windows NT 4.0 由於已不再推出修補程式，微軟網站上並無此系統的說明，可能亦存在此問題。

(二) 檢測方法

1.使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 19408 進行偵測，依此判斷是否存在此弱點。

2.使用微軟工具檢查

使用微軟的 MBSA 工具檢查此修補程式是否已安裝，或者使用 Windows Update 工具檢查是否已安裝此修補程式。

(三) 修補方式

下載 MS05-039 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/ms05-039.mspx

若是 Windows NT 4 的系統，因不再推出修補程式，建議更換新版作業系統。

此外更新方式亦可考慮使用 Windows Update 服務進行修補，若為多台主機情況，亦可使用 SUS 或 SMS 進行修補。

(四) 參考資料

微軟官方說明文件：

http://www.microsoft.com/technet/security/bulletin/ms05-039.mspx

CERT 弱點說明文件：

http://www.kb.cert.org/vuls/id/998653

四、 RealVNC 驗證方式可被規避弱點(Authentication Bypass Vulnerability)

(一) 簡要說明：

RealVNC 為廣泛使用的遠端管理工具，此工具分為 Client 與 Server 兩部份。其中 Client 藉由傳送帳號/密碼的方式，經由 Server 程式之驗證後。可進行安裝有 Server 程式系統之管理動作，其具有之權限通常為該系統之管理者權限(即 Windows 系統之 administrator 權限，或是 Unix 系統的 root 權限)，因此使用此系統之風險在於若設定之密碼不夠安全的話，將造成系統遭受誤用之風險大增。然

而於 2006 年 5 月時，此軟體被發現設計之疏忽與錯誤，使得即便已設定相對安全的密碼後，仍可能讓攻擊者可輕易規避程式之驗證過程，進而以系統管理者權限管理 RealVNC server 程式所在之系統。造成嚴重後果。

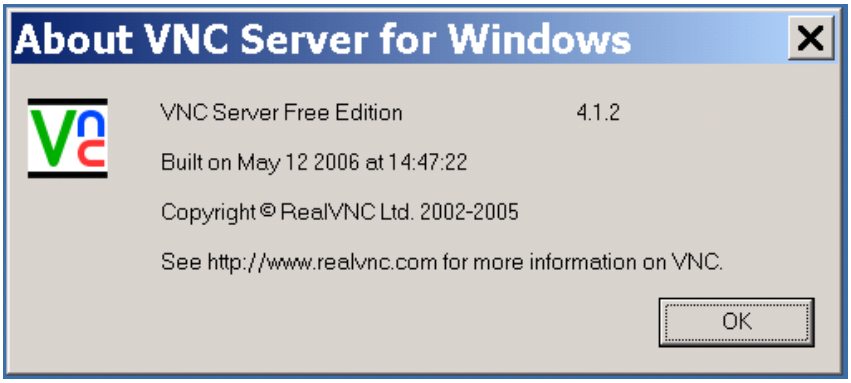
(二) 檢測方法

1. 使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 21564 進行偵測，依此判斷是否存在此弱點。若是 Nessus 系統上並無此 Plugin 存在，可能是未更新 Nessus 偵測 Plugin 造成之結果，還請執行/usr/local/sbin/nessus-update-plugins 指令更新，有關以上指令之進一步說明，可參考以下網址：http://www.nessus.org/plugins/

2. 由系統上直接檢查

若可直接登入安裝 RealVNC，亦可由系統上使用之版本直接檢查，例如以下版本為 4.1.2 版本，即為修正問題後之版本。



若為 Windows 系統，亦可由系統上之[新增移除程式]工具中驗證 VNC 之版本。其中若是 Free 版的 RealVNC 為 4.1.2 之前的版本，以及 Personal 與 Enterprise 版的 RealVNC 為 4.2.3 之前的版本的話，代表存在弱點，並且需要更新。至於 Unix Like 之系統，則請依據不同的系統套件檢查工具(如 rpm 或是 pkg_info 等等)進行檢查。

(三) 修補方式

請至官方網站(http://www.realvnc.com/)下載新版程式，並進行安裝並重新啟動即可，更新後並請再檢測是否已確實修正。

(四) 參考資料

http://lists.grok.org.uk/pipermail/full-disclosure/2006-May/046039.html

http://www.intelliadmin.com/blog/2006/05/security-flaw-in-realvnc-411.html

五、 Windows MSDTC 可讓攻擊者執行系統程式弱點或造成阻斷服務之弱點 (MS 06-018)

(一) 簡要說明：

MSDTC (Microsoft DataTransaction Coordinator)服務於 2006 年 5 月遭發現存在兩項弱點，其經由特殊設計之服務要求格式，可能導致 MSDTC 服務停止回應，造成阻斷服務情況，或是讓攻擊者得以成功入侵系統等兩項弱點。而 MSDTC 服務於 Win NT 4 與 Windows 2000 預設為啟動，而 Windows XP 及之

後的系統，預設為關閉，除非自行手動啟動。而其中又以 Win NT 4 與 Windows 2000 因可能經此弱點而遭入侵成功，以致情況較為嚴重，而 Windows XP 與 Windows 2003 則僅可能出現阻斷服務情況。

(二) 檢測方法

1. 使用弱點掃描軟體—Nessus 檢測

使用 Nessus 掃描軟體，並且使用 Plugin ID 21334 進行偵測，依此判斷是否存在此弱點。

2. 使用微軟工具檢查

使用微軟的 MBSA 工具檢查此修補程式是否已安裝，或者使用 Windows Update 工具檢查是否已安裝此修補程式。

(三) 修補方式

下載 MS06-018 的修補程式，網址為：

http://www.microsoft.com/technet/security/bulletin/ms06-018.mspx

若是 Windows NT 4 的系統，因不再推出修補程式，建議更換新版作業系統。

此外更新方式亦可考慮使用 Windows Update 服務進行修補，若為多台主機情況，亦可使用 SUS 或 SMS 進行修補。

(四) 參考資料

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0034

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1184

****

* **Revision**: 2006/3/31 version 1.0, 本版選定三項弱點，其中第一項為新增項目，其餘兩項為評估先前部分弱點後，經選定為本季之掃瞄項目

* 2006/5/22 Version 1.1, 本版因應 5 月出現兩項重大弱點，於評估研究後，於此版本增加此兩項弱點為編號第四點與第五點。

****