一、ASN.1 Parsing 弱點 (MS 04-007)

1. 簡要說明：

Abstract Syntax Notation 1 (ASN.1)為一資料處理標準，它已被許多應用程式用來處理不同平台間的資料正規化處理與互通，ASN.1 是一種用以定義資料標準的語言，亦即，資料處理的標準可用 ASN.1 撰寫。在 Microsoft 實作 ASN.1 時，由於實作上出現問題 (Buffer overflow)，導致可讓攻擊者遠端取得系統 System 帳號權限，造成攻擊者得以掌握受害系統。若要使攻擊成功，攻擊者需要使受害系統解析有問題的 ASN.1 資料，例如，若有以 ASN.1 為基礎的驗證協定，則攻擊者可能經由傳送惡意的驗證要求以期成功入侵系統。

2. 檢測方式：

由於 ASN.1 的實作上，Microsoft 將其應用在 HTTP server，Mail server 或 NTLM 驗證上，而在這些中，以 HTTP 部分的檢驗對於遠端掃描較可行並具代表性 (因使用 IIS server 的主機遠多於使用 Exchange server 的主機)，因此對於 IIS Server 進行弱點掃描之檢測工作，所使用的 Nessus 工具，而掃描所用的 plugin ID 為 12055。

3. 修正說明：

從 Windows NT 4.0 到 Windows 2003 皆有存在問題可能，其中 NT 4.0 在有安裝 MS 03-041 修正程式的前提下 (安裝後系統會存在 Msasn1.dll 檔案)，才會存在此問題，而其他的系統則是皆有此問題。對於有問題的系統，請安裝 MS 04-007 的修補程式，網址為：
http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx，或是使用 Windows Update 進行更新。

4. 參考資料：

http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx
http://support.microsoft.com/default.aspx?scid=kb;en-us;252648
http://cgi.nessus.org/plugins/dump.php3?id=12055

二、二十項相關國際認定重要弱點

請參考本中心網站上所公佈之說明及修補方式。網址為：
http://www.icst.org.tw/group/application/ncert/weak.php

請注意：只有 1、2、3、9 等四項是 Windows 2000 SP4 安裝後就可以修補的。目前掃描程式可能對第九項 – IIS 5.0 WebDAV overflow 弱點(MS03-007)有誤判的情形發生。如果您已確認安裝 SP4，請通知本中心將您的 IP 由名單中移除。

三、W32/Sasser 弱點 (MS 04-011)

1. 簡要說明：

W32/Sasser 是隻針對 Windows Local Security Authority Service Server (LSASS) 緩衝區溢位弱點所攻擊的網蟲。W32/Sasser 會隨機挑選 IP 位址，試著去掃描主機是否為開啟 port 445 的 windows 平台，探測主機是否存在 LSASS 的弱點，若有則進行感染散播。而尚未修補弱點的主機會在網蟲探測感染後，會導致 LSASS.exe 程序執行異常，Windows 會顯示一分鐘後關機的警訊。

受影響平台：

Windows NT
Windows 2000
Windows 2003

2. 檢測方式：

(1)檢查主機是否已遭 W32/Sasser 感染

W32/Sasser 為了每次開機都會自動被執行，會在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 加入一登錄值，avserve.exe。若有此登錄值，表示該主機已遭 W32/Sasser 感染。

(2)檢查主機是否有 LSASS 弱點

檢查主機是否存在 LSASS 弱點，可用 Nuessus 做外部掃描，掃描的 plugin ID 為 12209。

3. 修正說明：

(1) 若已遭 W32/Sasser 感染

若經上述的檢測方式確定主機已遭 W32/Sasser 感染，請至 Symantec 下載病毒移除工具 FxSasser.exe，下載網址，http://securityresponse.symantec.com/avcenter/FxSasser.exe，病毒移除工具的使用方式請參考 Symantec 的說明文件，http://www.symantec.com/region/tw/avcenter/vinfo/venc/data/tw-w32.sasser.removal.tool.html。

(2) 修補 LSASS 弱點

LSASS 的弱點已在微軟的安全性公告 MS04-011 (http://www.microsoft.com/taiwan/security/bulletins/ms04-011.asp) 有相關描述，微軟也提供修補程式，在 MS04-011 有提供下載的連結，請使用者根據自己作業系統的版本與語系下載適合的修補程式安裝，或是使用 Windows Update 進行更新。MS04-011 除了修正 LSASS 弱點外，還修正了其他微軟作

業系統平台的安全性問題，詳細資料請參閱 MS04-011。

4. 參考資料：

Microsoft 安全性公告 MS04-011
http://www.microsoft.com/taiwan/security/bulletins/ms04-011.asp
Sasser 蠕蟲的常見問題集
http://www.microsoft.com/taiwan/security/incident/sasserfaq.asp
Symantec 安全威脅 - W32.Sasser.Worm
http://www.symantec.com/region/tw/avcenter/vinfo/venc/data/tw-w32.sasser.worm.html
Symantec - W32.Sasser 移除工具
http://www.symantec.com/region/tw/avcenter/vinfo/venc/data/tw-w32.sasser.removal.tool.html