



首廿大嚴重安全弱點 專家們的共同建議

5.0 版，2004 年 10 月 8 日

Copyright (C) 2001-2004, SANS Institute
請將您的疑問與意見寄至 top20@sans.org.

-----前往首廿大威脅目錄索引-----

簡介

SANS 首廿大網路安全弱點

大多數網蟲與電子攻擊都是利用常用作業系統上的服務程式漏洞。攻擊者最喜歡見縫插針，他們選擇最為簡易方便的手法，亦即使用效果最好且廣為流傳的攻擊工具來攻擊著名系統弱點。他們看準了公司組織不會馬上去修補這些問題，因此採取無差別攻擊方式掃瞄整個網際網路來尋找受害系統。

四年前，SANS 協會(SANS Institute)與聯邦調查局(FBI)的國家基礎設施保護中心(NIPC)發布了一份文件，整理出前十大嚴重的網路安全弱點，並在接下來的幾年內增列成首廿大安全弱點列表。數以千計的組織都參考這份文件，讓管理者們能夠優先對最嚴重的漏洞進行修補。引發 Blaster、Slammer、Code Red 及 NIMDA 等網蟲的弱點原兇都名列榜上。

SANS 2004 年首廿大網路安全弱點列表其實包含了兩個前十大列表：前十大 Windows 系統上最常見的弱點，及前十大 UNIX 系統與 Linux 系統上最常見的弱點。雖然這些系統上每年均發生數以千計的資安事故，但被攻擊成功的受害成因幾乎都包含於這份首廿大列表中。

這份列表依嚴重性列出了需要立即修補的弱點，這是一群首席安全專家合作的成果。他們來自對安全性極端敏感的英、美及新加坡政府單位、安全軟體廠商龍頭與顧問公司、頂尖的安全研究學術單位、及許多其他使用者組織和 SANS 協會。文件未列出了所有參與成員。

SANS 首廿大列表是個永不停息的文件。它包含了關於弱點修補的詳細步驟、指令與進一步的有用參考資訊。一旦發現更嚴重的威脅、更立即或更方便的保護方式，我們會更新這些列表及修補說明，我們也歡迎您的加入，這是一份屬於大眾的文件 -- 你對於抵禦攻擊者及清除弱點的經驗可以幫上其他人。請將您的建議寄到 top20@sans.org

前十大 Windows 系統上的弱點

- W1 網頁伺服器與服務
- W2 Workstationz 服務
- W3 Windows Remote Access 服務
- W4 Microsoft SQL Server (MSSQL)資料庫
- W5 Windows 身分驗證
- W6 網頁瀏覽器
- W7 檔案共享應用程式
- W8 LSAS 漏洞
- W9 收信軟體
- W10 即時通訊

前十大 UNIX 系統上的弱點

- U1 BIND 域名系統
- U2 網頁伺服器
- U3 身分驗證
- U4 版本控制系統
- U5 郵件傳送服務
- U6 簡單網路管理協定 (SNMP)
- U7 開放式安全傳輸層協定 (SSL)
- U8 企業服務 NIS/NFS 的錯誤設定
- U9 資料庫
- U10 系統核心

Windows 系統上的重大弱點(W)

W1. 網頁伺服器與服務(Web Servers & Services)

W1.1 說明

Windows 平台上各種 HTTP 伺服器的預設安裝選項，及預設附加的各種服務元件等（像是串流影音多媒體協定）均眾所周知地漏洞百出。這些弱點所造成的影響包含：

- 阻絕服務(Denial of service)
- 機密檔案或資料外洩
- 可於受害主機上執行任意指令
- 受害主機被完全佔領

包含 IIS、Apache 及 iPlanet(現在的 SunOne)在內的 HTTP 伺服器都具有多個已發布修補程式的弱點，請確認服務中主機都已更新所有修補程式。多數 HTTP 伺服器的預設設定選項都為入侵者大開方便之門。雖然 IIS 6.0 已經改變態度提供「安全的預設選項」概念，但是對管理者們來說，要完全瞭解手上的網頁伺服器，並有能力調整設定只開放必需功能與服務，仍是件辛苦且耗時甚鉅的工作。

IIS 使用了稱為 ISAPI 的程式掛勾(hook)方式，將某些副檔名關聯至相應的動態連結資料檔(DLL)，這些程式稱為 ISAPI 擴充程式。ColdFusion、使用 ISAPI 的 PHP、IIS 等前置處理器中都包含了許多 ISAPI 擴充程式，用以處理動態伺服頁(ASP)、.NET 網頁服務及網頁式共享列印。許多與 IIS 5.0 及之前版本一起預設安裝的 ISAPI 擴充程式其實都不是必要功能，而其中的過濾器多數都可被入侵。利用這些問題造成大量繁衍的惡意程式範例包含了著名的 Code Red 與 Code Red 2 網蟲。我們建議只開啓網頁伺服器所需辨識的 ISAPI 擴充程式，並限制可使用這些 ISAPI 擴充程式的 HTTP 要求訊息選項。採用微軟免費提供的 IIS LockDown 工具是最佳的安全強化措施。

大多數網頁伺服器都含有範例程式或網頁，用以展示該網頁伺服器的功能。這些範例程式並未考量在真實環境中的安全性。IIS 6.0 之前的版本就包含了許多可被侵入的範例程式，可被遠端瀏覽或覆寫任意檔案，甚至讓人遠端存取其他重要資訊，像是系統設定與程式路徑。請在將伺服器上線之前先移除這些範例程式。

安裝之後並未定期維護的網頁伺服器也是新舊弱點的大本營。例如微軟安全公告 MS04-011 中所提及的 PCT 與 SSL 弱點，就會造成阻絕服務或讓攻擊者取得主機權限。持續修補公開提供服務的伺服器是絕對必要的。

第三方組織所提供的網頁增益元件，像是 ColdFusion 與 php，在隨網頁伺服器安裝時都曝露了更多弱點，包含使用者的錯誤設定與元件產品本身的弱點。

W1.2 受影響的作業系統：

任何安裝了網頁伺服器的微軟 Windows 系統都受到影響。這包含了（但不僅只於）以下系統：

- Microsoft IIS：Windows NT4.0 及之後版本，包含 XP Professional
- Apache HTTP 伺服器：Windows NT4.0 SP3 及之後版本均可支援，雖然咸認它也可以在 Win95 與 Win98 上執行
- Sun Java System/Sun One/iPlanet 網頁伺服器：Windows NT4.0 SP6 及之後版本

*請注意：*Windows 2000 Server 的系統預設安裝即包含了 IIS，許多管理者在著名的 Nimda 與 Code Red 網蟲事件後才發現這點。在實作高可信度電腦運算(Trustworthy Computing)的前提下，Windows Server 2003 的標準安裝中不啓用 IIS 伺服器，其預設設定亦以安全為優先考量。此外，某些第三方應用程式需要 IIS 所提供的功能，若管理者在安裝這些軟體並未留意，也會同時啓用 IIS。千萬不要以為不主動安裝網頁伺服器就不會遭受網頁攻擊，請定時尋找並稽核現存網路上未經許可的網頁伺服器。可參閱下面「如何得知你是否具有這類風險」一節。

W1.3 相關的 CVE/CAN 項目

a. IIS [CAN-2003-0225](#), [CAN-2003-0377](#), [CAN-2003-0227](#), [CAN-2003-0349](#), [CERT-VU-288308](#), [Secunia-12647](#), [Secunia-12638](#), [Secunia-11563](#)

可搜尋關於 IIS 2.0 的 [CVS 項目](#)、關於 IIS 3.0 的 [CVS 項目](#)、關於 IIS 4.0 的 [CVS 項目](#)、關於 IIS 5.0 的 [CVS 項目](#) 及關於 IIS 6.0 的 [CVS 項目](#)。

b. Apache

[CAN-2003-0987](#), [CAN-2003-0842](#), [CVE-2004-0009](#), [CVE-2004-0113](#), [CVE-2003-0993](#), [CAN-2004-0174](#), [CAN-2004-0492](#), [CAN-2004-0488](#), [CAN-2004-0748](#), [CAN-2004-0700](#), [CAN-2004-0751](#), [CAN-2004-0809](#), [CAN-2004-0786](#), [CAN-2004-0811](#)

[CVE-2003-0016](#), [CVE-2003-0017](#), [CAN-2003-0460](#), [CAN-2003-0844](#), [CAN-2004-0493](#)

Apache 模組：[CAN-2003-0844](#), [CAN-2004-0492](#)

c. iPlanet/Sun

[CAN-2003-0411](#), [CAN-2003-0412](#), [CAN-2003-0414](#), [CAN-2003-0676](#)

[CAN-2002-1315](#), [CAN-2002-1042](#), [CVE-2002-0845](#), [CAN-2003-0676](#)

d. 增益元件

[CAN-1999-0455](#), [CAN-1999-0477](#), [CAN-1999-1124](#), [CAN-2001-0535](#), [CAN-2001-1120](#), [CAN-2002-1309](#), [CAN-2003-0172](#)

[CVE-1999-0756](#), [CVE-1999-0922](#), [CVE-1999-0924](#), [CVE-2000-0410](#), [CVE-2000-0538](#)

ColdFusion: [CAN-2002-1309](#), [CAN-2004-0407](#), [CVE-2000-0189](#), [CVE-2000-0382](#), [CVE-2000-0410](#), [CVE-2000-0538](#), [CVE-2002-0576](#)

PHP: [CAN-2002-0249](#), [CAN-2003-0172](#)

e. 其他服務

[CAN-1999-1369](#), [CAN-2003-0227](#), [CAN-2003-0349](#), [CAN-2003-0725](#), [CVE-2003-0905](#)

[CVE-1999-0896](#), [CVE-1999-1045](#), [CVE-2000-0211](#), [CVE-2000-0272](#), [CVE-2000-0474](#), [CVE-2000-1181](#), [CVE-2001-0083](#), [CAN-2001-0524](#)

W1.4 如何得知你是否具有這類風險

任何使用預設安裝或未經修補的網頁伺服器都應被視為具有弱點。

多數網頁伺服器或服務廠商都提供了與安全事務相關的豐富資訊，以下是一些範例：

- Apache HTTP 伺服器 [首頁](#) 及 [安全報告](#)。
- 微軟 [TechNet 技術網路安全中心](#)
- 微軟 [IIS 安全中心](#)
- Sun [網頁、入口與目錄伺服器下載中心](#)
- [Macromedia 安全地帶](#)
- [Real Networks 安全事務](#)
- [PHP 首頁](#) 與 [下載區](#)。

也請隨時確認網頁伺服器及相關服務的修補更新版本和設定檔，定期瀏覽廠商與 [CVE 資料庫](#) 所提供的安全資訊，以評估可能具有的潛在弱點。新的安全問題不斷被發現，最好的因應方式就是善用微軟的 [Windows 更新網站](#)、[Microsoft Security Baseline Analyzer](#) 及 [自動更新](#) 功能以清除潛在弱點。

遠端或本機型的弱點稽核工具也可以幫助網頁伺服器管理者稽核他們的網路，這些工具包括：

- [Nessus](#) (開放原始碼軟體)
- [SARA](#) (開放原始碼軟體)
- [Nikto](#) (開放原始碼軟體)
- [eEye 免費工具](#) 及 [商用掃描軟體](#)。
- [Microsoft Baseline Security Analyzer](#) (含有許多針對 IIS 作稽核的安全功能)。

建議使用遠端弱點稽核工具對整個網路進行掃描，這會比針對已知主機進行稽核來得有效率，因為可以找出網路內未經許可的網頁伺服器，並稽核其潛在弱點。

W1.5 如何針對弱點進行防護

對多數系統來說

1. 除了 HTTP 伺服器本身外，同一主機上的作業系統及其他應用程式也必需安裝最新的服務套件(Service Pack)與安全更新程式。更新後，建議再開啓 [自動更新](#) 功能以啓用最高安全等級保護。
2. 安裝主機型防毒及入侵偵測軟體。兩者都需持續更新，並經常檢視其記錄檔。
3. 關閉不需要使用的腳本程式直譯器，並移除它們的執行檔。例如：`perl`、`perlscript`、`vbscript`、`jsript`、`javascript` 及 `php`。
4. 如果可以啓用記錄功能，請啓用並隨時檢視記錄檔。更甚者，還可透過自動程式統計事件並回報異常或可疑活動。
5. 使用 `syslog` 類的系統將作業系統與 HTTPd 記錄檔安全儲存於其他主機。
6. 攻擊者常用一些系統工具協助發動初步入侵或擴展戰果，請移除或限制這些工具的使用。像是 `tftp(.exe)`、`ftp(.exe)`、`cmd.exe`、`bash`、`net.exe`、`remote.exe`、及 `telnet(.exe)`。
7. 限制在 HTTP 服務/常駐程式(daemon)及輔助服務執行主機上的其他應用程式。
8. 注意並減少任何服務廠商利用公開網頁伺服器與內部網路接觸的機會。例如設定對 NetBIOS 分享或信任關係。
9. 公開系統及內部系統需使用不同的帳號命名規範及獨立密碼。不能讓任何公開系統可能洩露出的資訊造成對內部系統的危害。

a. IIS

請考慮將你的 IIS 更新到 IIS 6.0 版，可大幅提昇安全性。修補伺服器是當務之急，但卻不是僅此而已。當新的 IIS 弱點被發現時，請同步進行修補。對單機伺服器來說，可以選擇使用 [Windows 更新](#) 網站及 [自動更新](#) 功能。對於管理整個環境、或負責多個分散式系統的管理者來說，[系統管理伺服器 \(SMS\)](#) and [軟體更新伺服器 \(SUS\)](#) 也是很好的選擇。[MBSA](#) 是微軟提供的網路端安全修補程式檢查器，可以協助系統管理者掃描本機或遠端系統的更新狀態。這個工具可支援 Windows NT 4、Windows 2000、Windows XP 與 Windows 2003。最新版本可由微軟網站下載，網址為：<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

使用 IIS Lockdown Wizard 來強化安裝流程

微軟發布了一支可以協助強化 IIS 安裝流程的簡易工具，稱作 IIS Lockdown Wizard。最新版本可由微軟網站下載，網址為：<http://www.microsoft.com/technet/security/tools/locktool.asp>

在「custom」或「expert」模式下執行 IIS Lockdown Wizard，可以對下列的 IIS 建議設定進行調整：

- 確認伺服器上安裝了最新版的 WebDAV。IIS 6.0 可以讓管理者選擇是否啓用 WebDAV。
- 取消所有非必需 ISAPI 擴充程式的關聯對應(包含了 .htr、.idq、.ism 等，特別是 .printer)。
- 清理範例程式。
- 限制網頁伺服器上最常被利用於攻擊及入侵的相關程式權限及可用性(例如 cmd.exe 與 tftp.exe)。

SANS 讀書間裏收錄了〈[瞭解及安裝 IISlockdown 工具](#)〉以及〈[Windows 2000 IIS Web Server 安全教學](#)〉。[微軟安全中心](#)則收錄了完整詳細的設定指示，教你如何保護及管理 IIS。

使用 URLScan 來過濾 HTTP 要求訊息

包含 Code Blue 與 Code Red 系列在內的許多 IIS 攻擊程式都會使用惡意的 HTTP 要求訊息，來達成目錄跳脫(directory traversal)與緩衝區溢位(buffer overflow)攻擊。利用 URLScan 過濾器元件進行設定，就可以在伺服器處理這些要求訊息前先行拒絕它們。最新版的 URLScan 已整合於 IIS Lockdown Wizard 內，可由微軟網站下載，網址為：<http://www.microsoft.com/technet/security/tools/urlscan.mspx>。

b. Apache

關於在 Apache 伺服器上設定存取控制、IP 限制、使用 Apache 安全模組及其他與安全相關的設定方式與討論，都可在 [Apache 教學](#) 網頁中找到。

除此之外，由 Artur Maj 所寫的〈[一步步保護 Apache 安全](#)〉也是一份很有用的文件，可以協助對 Apache 伺服器進行詳細的安全設定。這份文件可以在 SANS 讀書間找到。

c. iPlanet/Sun One

Edmundo Farinas 在他的文章〈[Solaris 上 iPlanet Enterprise 網頁伺服器的安全考量](#)〉中說明了 iPlanet 的安全設定，亦可在 [SANS 讀書間](#) 找到。

另外，Sun 提供了〈[Sun ONE 應用伺服器安全目標](#)〉文件，詳細記載了保護 iPlanet/Sun One 伺服器的詳細步驟。

d. 增益元件

如果使用了第三方組織的增益元件，像是 ColdFusion、PerlIIS 或 PHP，請瀏覽供應廠商的網頁以檢
索修補程式和設定方式。理由顯而易見，微軟不會在 [Windows 更新](#) 上提供第三方軟體更新程式。

與 ColdFusion 安全相關的安全資訊可參閱 SANS 讀書間中，Joseph Higgins 所寫的文件 [〈網頁應用
程式安全：ColdFusion 篇〉](#)。

Artur Maj 所寫的 [〈一步步保護 Apache 安全〉](#) 描述了強化 PHP 應用程式的流程，本文收錄於 [SANS
讀書間](#)。

另外，[〈PHP 手冊第十六章〉](#) 對 PHP 安全設定也很有幫助。

e. 其他服務

上述建議只是對網頁伺服器的一般安全防護步驟，各軟體供應廠都有提供各自的更新及修補方式、
建議設定選項及記錄功能。

檢視軟體廠商網站上的相關文件，並登記加入各廠商的信件通知服務與電子報。這可以讓你即時得
知最新的安全問題，以求在第一時間內有效率地進行處理。

[回頁首 ^](#)

W2. Workstation 服務(Workstation Service)

W2.1 說明

Windows Workstation 服務負責處理使用者對資源的存取需求，例如檔案或印表機。這個服務程式
會檢查所需資源是存在於本機還是網路分享，並將使用者的要求導向相應位址。

這個服務所提供的網路管理函數可被下列機制所呼叫：

- DCE/RPC 在連結使用 \\pipe\wkssvc 的命名管線呼叫(named pipecall)服務程式後，會呼叫
SMB 協定。
- DCE/RPC 直接呼叫 UDP 連接埠(埠號>1024)
- DCE/RPC 直接呼叫 TCP 連接埠(埠號>1024)

注意，這個服務程式會綁用大於 1024 後，第一個可用的 TCP 或 UDP 埠號。

送出特製的 DCE/RPC 呼叫，可觸發 Workstation 服務中一個堆疊緩衝區溢位問題，這是因為程式並
未對傳至記錄函數的參數大小進行檢查。未經身分驗證的遠端攻擊者可藉由這個溢位問題侵入
Windows 主機，並在受害主機上以「SYSTEM」權限執行任意程式，從而獲得主機的完整權限。針
對此漏洞所撰寫的攻擊程式已被公布於網路上，並被 Phatbot/Gaobot 網蟲的各式變種版本重覆利
用，感染了數百萬台系統。

W2.2 受影響的作業系統：

Windows 2000 SP2, SP3 與 SP4

Windows XP, Windows XP SP1

Windows XP 64 位元版本

W2.3 CVE/CAN 項目

[CAN-2003-0812](#), [CAN-2003-0813](#), [CAN-2003-0352](#)

W2.4 如何得知你是否具有弱點

未更新過 MS03-049 的 Windows 2000 系統，及未更新 MS03-043 的 Windows XP 系統都具有此弱點。更新至 Service Pack 2 的 Windows XP 使用者則不受影響。

檢查下列登錄值(registry)：

KB828035: 在 HKLM\Software\Microsoft\Updates\Windows XP 下 (Windows XP 環境)

KB828749: 在 HKLM\Software\Microsoft\Updates\Windows 2000 下(Windows 2000 環境)

如果 Windows 系統中不具有這些登錄值，則你的主機可能具有弱點。想要進一步確認以降低風險，可使用安全掃描軟體，例如 Microsoft Baseline Security Analyzer (MBSA)，來檢查是否已更新相關修補程式。MBSA 可由下列網址下載：

<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

W2.5 如何進行保護

- a. Windows XP Service Pack 2 提供許多安全補強功能以因應資安風險。**US-CERT** 建議應於安裝 Windows XP 時列入優先考量。
- b. 要確保 Windows 系統已安裝最新版的安全修補程式與服務套件。無論是個人使用或公司主機，都應將啟用**自動更新**選項視為必要工作。要特別檢查 Windows 2000 系統是否已更新 MS03-049、Windows XP 系統是否已更新 MS03-043。總而言之，Service Pack 2 應被考慮為必要安裝的更新程式。
- c. 在網路邊境上阻擋 139/tcp 與 445/tcp 封包進入，可以防止遠端攻擊者使用 SMB 進行攻擊。
- d. 對於 1024 以上的埠號，在網路邊境上只開啓必需的 TCP 連接埠。這可以防止遠端攻擊者使用 DCE/RPC 呼叫進行溢位攻擊。注意，要在防火牆上阻擋 1024 以上的 UDP 埠號是極困難的，因為這個範圍的埠號經常被作為暫用埠號。
- e. 使用 Windows 2000 與 XP 上內建的 TCP/IP 篩選器，或 Windows XP 系統內建的 Windows 防火牆來阻擋意圖內送存取上述埠號的封包。Windows 防火牆亦可讓網路管理者能集中控管終端使用者系統，以協助提升系統安全性。
- f. 對於在自行調整後的 Windows 2000/XP 上執行的第三方應用程式，請確保它們都已安裝廠商所提供的修補程式。舉例而言，思科(Cisco)發布了一個公告，描述數個思科產品會受此弱點影響，並已提供修補程式。
- g. 如果系統是獨立運作的主機（亦即不屬於任一 Windows 網路），則可直接停用 Workstation 服務。要注意的是，這樣作可能會影響某些應用程式或系統功能。

進一步資訊：

微軟公告

<http://www.microsoft.com/technet/security/bulletin/MS03-049.mspx>

eEye 通報

<http://www.eeye.com/html/Research/Advisories/AD20031111.html>

CERT 通報

<http://www.cert.org/advisories/CA-2003-28.html>

<http://www.kb.cert.org/vuls/id/567620>

CORE 安全通報

<http://archives.neohapsis.com/archives/vulnwatch/2003-q4/0066.html>

思科通報

<http://www.cisco.com/warp/public/707/cisco-sa-20040129-ms03-049.shtml>

W3. Windows Remote Access 服務(Windows Remote Access Services)

W3.1 說明

Windows 作業系統家族支援各種不同的網路模式與技術，原始設計中就同時支援產業上的標準網路通訊協定及內建的微軟專屬網路模式與技術。其網路分享、匿名登入、遠端存取登錄值(remote registry access)及遠端程序呼叫(RPC)等功能都提供了可入侵的管道。

NETBIOS - 一組應用程式設計介面(API)，可允許不同主機利用 Windows 網路共享以橫跨網路來分享檔案或檔案夾。此功能底層的基本機制為服務訊息區塊協定(Server Message Block, SMB)或共用網際網路檔案系統(Common Internet File System, CIFS)。這些協定允許系統如同本機檔案般地操作遠端檔案。

雖然這是 Windows 一個強大且有用的功能，但網路分享設定不當，可能將許多重要系統檔案曝露在外，使得惡意使用者或程式得以完全控制主機。其中一個方式被 I-Worm.Klez.a-h (**Klez 系列**)網蟲、Sircam 病毒(參閱 [CERT 通報 2001-22](#))與 Nimda 網蟲(參閱 [CERT 通報 2001-26](#))所採用。它們將惡意程式置放到未受保護的網路檔案夾，因而得以在 2001 年快速散布。許多電腦使用者為了方便工作夥伴，將磁碟的讀寫權限開放給網路使用者，也就因此無意間將系統開放給了駭客。

匿名登入 - 匿名連線指的是在未提供正確身分識別時所建立而成的通訊連線，例如使用空白帳號或密碼。空連線(Null session)可用以探查使用者、使用群組、檔案共享與密碼規則等資訊。微軟 Windows NT 系統中以 Local System 身分執行的本機服務程式就是以空連線的方式與其他網路主機進行通訊。Windows 2000 之後的主機服務則會使用本機帳號進行驗證。

遠端存取登錄值 - 微軟 Windows 9x、Windows CE、Windows NT、Windows 2000、Windows 2003、Windows ME 與 Windows XP 都佈屬了一個中央階層式資料庫，被稱為登錄值(Registry)。登錄值被用於軟體、裝置及使用者設定。不當的安全或存取權限設定都可讓遠端使用者直接存取登錄值，甚至執行不被允許的程式或軟體。

遠端程序呼叫 - 所有版本的微軟作業系統(Windows NT 4.0、2000、XP 與 2003)都提供了內部程序通訊機制，以讓本機程式可於遠端主機上執行。三個可讓使用者利用 Local System 權限執行任意程式的相關弱點已經公布，其中之一被 Blaster/MSblast/LovSAN 與 Nachi/Welchia 網蟲所利用。還有一些其他弱點可讓攻擊者針對 RPC 元件發動阻絕服務攻擊(Denial of service)。

W3.2 受影響的作業系統：

Windows 95、Windows 98、Windows NT Workstation 與 Server、Windows Me、Windows 2000 Workstation 與 Server、Windows XP Home 與 Professional、以及 Windows 2003 全都具有潛在弱點

Windows XP Service Pack 2 修改了 **RPC 行為模式**，它在預設設定中實作了新的 RPC 限制介面，使得系統更加安全。值得一提的是它新增了一個登錄值 - RestrictRemoteClients。這個登錄值修改了系統上所有 RPC 介面的行為，並預設清除了對 RPC 介面的遠端匿名存取權限，有效移除了這類風險。

W3.3 CVE/CAN 項目

NETBIOS

[CVE-2000-0979](#) (只適用於 Windows 95, 98, 與 Windows Me), [CAN-2003-0661](#)

[CAN-1999-0518](#), [CAN-1999-0519](#), [CAN-1999-0621](#), [CAN-2000-1079](#)

匿名登入

[CVE-2000-1200](#)

遠端存取登錄值

[CAN-2000-0377](#), [CVE-2002-0049](#)

[CAN-1999-0562](#), [CAN-2001-0045](#), [CAN-2001-0046](#), [CAN-2001-0047](#), [CVE-2002-0642](#), [CVE-2002-1117](#)

遠端程序呼叫

[CAN-2002-1561](#), [CVE-2003-0003](#), [CAN-2003-0352](#), [CAN-2003-0528](#), [CAN-2003-0605](#), [CAN-2003-0715](#), [CAN-2001-0509](#), [CAN-2003-0813](#)

W3.4 如何得知你是否具有弱點

如何得知你是否具有與 NETBIOS 相關的弱點

有幾種工具可以幫助你知道系統上是否具有 NETBIOS 相關的弱點。

NbtScan - NetBIOS 網路名稱掃描，可以檢查目標系統上是否開啓檔案共享服務。NbtScan 可由此下載：<http://www.inetcat.org/software/nbtscan.html>。

NLtest - 極爲強大的工具，收錄於 [Windows 2000 與 2003 輔助工具包](#) (在產品光碟裏)及 [Windows NT4 資源工具包\(NTRK\)](#) 中。NLtest 可獲取許多與潛在設定弱點有關的資訊。

[Microsoft Baseline Security Analyser](#) 會回報 Windows NT (SP4)、Windows 2000、Windows XP 及 Windows 2003 系統是否容易被 SMB 攻擊手法入侵，好讓管理者能夠修正問題。這個工具可於本機測試，也可用於遠端主機。

Windows NT、Windows 2000、Windows XP 及 Windows 2003 的使用者可藉用在命令提示字元下鍵入簡單的「net share」指令來檢查自己分享了哪些資源。要知道 net share 的進一步用法，請鍵入

```
net share /?.
```

特別注意：本文描述修改共享資源的資訊。在修改共享資源前，請確定如果發生問題時，你知道如何回復這些資源。我們建議對正在運作的主機進行修改前，都要先行測試。想知道與共享資源相關的資訊，請點擊下列文章，看看微軟知識庫中怎麼說：

[125996 - 儲存及回復現有的 Windows 共享](#)

[308419 - 如何設定、檢視、變更或移除 Windows XP 檔案和資料夾的特殊使用權限](#)

[307874 - 如何在 Windows XP 的共用資料夾停用簡易的共用並設定使用權限](#)

[174273 - 如何複製檔案、維護 NTFS 及共享權限](#)

設定檔案系統權限應列爲優先考量，網路共享資源的預設權限如下：

Windows NT、Windows 2000 與 Windows XP (Service Pack 1 之前)

- Everyone - 完全控制

Windows XP SP1

- Everyone - 讀取

預設分享一個叫作「SharedDocs」的資料夾，它的實體對應位址為

C:\Documents and Settings\All Users\WINDOWS

- 檔案與資料夾的擁有者及本機管理者具有讀取及寫入權限，其他人則沒有讀取或寫入權限。這是每個使用者的「我的文件」資料夾的預設設定。

大多數商用網路掃描軟體都可以偵測到你是否開放共享資源。可以利用 [Gibson Research Corporation 網站](#)所提供的方式來進行快速又有效的 SMB 探查測試，不過其精準度要看目標主機是否被防火牆或任何遮蔽設備所保護。

下面是一些可用於偵測共享弱點的自動掃描工具：

- [Nessus](#)--免費、強大、更新快且易用的網路掃描軟體
- [vacuum](#) 寫的 [Winfingerprint](#) --列舉 Win32 主機/網路的掃描軟體
- [Microsoft Baseline Security Analyser](#) - 免費的網路安全工具

如何得知你是否具有與匿名登入相關的弱點。

可由命令提示字元下試著對目標主機建立空連線：（開始 --> 執行 --> 鍵入 cmd）：

```
C:>net use \\目標主機 IP\ipc$ "" /user:""
```

上述指令可使用空白密碼連結到一個隱藏的內部程序：「在目標主機 IP 上利用空白使用者(user: "") 開放的 IPC\$ 共享」。

如果收到「命令執行成功。」，則代表目標主機可能可由遠端採集資訊及列舉帳號。

包含 Nessus 與 Winfingerprint 在內的上述工具均可用於偵測空連線(null session)的弱點。

如何得知你是否具有與遠端存取登錄值相關的弱點

透過正式管道由微軟取得的 Windows NT 資源工具包(NTRK)中有一個叫作 Regdump.exe 的執行程式，可讓你由 Windows NT 主機對網際網路或內部網路上其他 Windows NT/Windows 2000/Windows XP 主機進行測試，看看是否可以存取它們的登錄值。

另外也有一些命令列程式可用於測試登錄值存取權限及其他安全問題，請由此下載：

<http://www.afentis.com/top20>.

如何得知你是否具有與遠端程序呼叫相關的弱點

微軟已經發布一個可以檢查修補程度、設定方式與修補層級的工具，並供免費下載，這是找出 Windows 主機是否受弱點影響的最好方式。這個工具叫作 Microsoft Baseline Security Analyzer (MBSA)，可由下列網址下載：<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

CAN-2003-0352、CAN-2003-0528、CAN-2003-0605 與 CAN-2003-0715 等弱點也具有專屬的掃描工具，可幫助檢查是否進行了對應的修補，請由此下載：<http://support.microsoft.com/?kbid=827363>。然而我們還是建議使用 MBSA，因為它涵蓋的範圍較廣。家用主機或主機不多的使用者可以直接為每台主機進行更新與檢查，請造訪 Windows 更新網站：<http://windowsupdate.microsoft.com/>

W3.5 如何針對弱點進行防護

微軟會為每個作業系統或應用程式弱點發布服務套件(Service Pack)或修補程式，請一定要讓你的系統套用最新的服務套件。以 Sasser 網蟲為例，它及它的變種(利用 LSASS 系統弱點)曾經感染世界上許多未進行修補的主機，而安裝了 MS04-011 修補程式的系統就得以免於受害。微軟在 Sasser 網蟲出現的幾週前就已釋出 MS04-011 的修補方式。

注意：微軟已不再維護與支援 Windows 95 與 Windows NT4 Workstation。對 Windows NT4 Server 的支援也直到 2004 年 12 月 31 日。

想知道關於作業系統的生命週期，請參閱微軟文件：〈[Windows 系列的產品產品週期時程](#)〉。

要為系統尋找相關安全修補程式，請利用：

- [Windows 更新](#)服務它可以自動偵測系統所需要的安全修補程式，並在點選確認後自動安裝。
- 啟用[自動更新](#)功能以強化微軟作業系統與應用程式。
- [Windows 安全公佈欄線上搜尋服務](#)，位於：
<http://www.microsoft.com/technet/security/current.aspx>

安裝最新的服務套件與修補程式可以解決很多軟體上的問題（像是緩衝區溢位、程式設計錯誤等），但 Windows 作業系統中仍有許多已載明的危險功能應被關閉，以強化系統安全性。要瞭解並找出潛在的安全問題或風險，請採用 [Microsoft Baseline Security Analyzer \(MBSA\)](#)。

如何針對 NETBIOS 相關弱點進行防護

你可以採取某些行動來降低微軟網路漏洞所曝露出的弱點。注意：在關閉資源分享或 NETBIOS 功能時要特別提高警覺，以免反向影響到企業正常提供的應用程式與服務。在修改正在運行中的系統前，要確認每項變更行為都經過完整測試。

如果你的系統不需提供檔案/列印服務，且不需要讓人進行遠端管理（大多數家用主機都屬於此類），則可關閉 Server 服務。

在 Windows NT4/2000/2003/XP 系統上，可由下列步驟停用 Server 服務：開始 - 設定 - 控制台 - 系統管理工具 - 服務 - 選擇 Server 服務 - 雙擊 - 將啟動類型改為「停用」 - 點擊「套用」 - 點擊「停止」 - 點擊「確定」。

如果你的系統需要 Server 服務，則建議依[微軟安全導引中心](#)的最佳設定實務來進行設定。除此之外，下面這些步驟也可以幫助加強 Windows NT4/2000/2003/XP 系統的安全：

1. 列舉所有預設隱藏共享資源(C\$, D\$, E\$等)，請在系統命令提示字元下鍵入指令：

```
net share
```

記下列出的所有共享資源。

2. 移除預設的隱藏共享資源。注意，移除隱藏共享資源常常會導致企業正常提供的應用程式無法正常執行，像是備份與管理用的應用程式。要確保重開機後這些隱藏共享資源仍保持移除狀態，就必需對登錄值進行調整(步驟稍後列出)。要移除隱藏共享資源，請在系統命令提示字元下鍵入指令：

```
net share C$ /delete
```

在大部分情形下，以英文字為名的共享資源(C\$、D\$、E\$等)及 ADMIN\$皆可被正常移除，不建議移除任何系統上的預設 IPC\$ 共享。

3. 重新開機或重新啓動 Server 服務後，被移除的預設共享就會自動回復為開啓狀態。想要永久移除它們，就必需修改登錄值：
 - 開啓登錄編輯器
 - 尋找登錄值：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
 - 在其下新增一組登錄值
 - 登錄名稱：AutoShareWks
 - 登錄類型：DWord
 - 登錄數值：00000000
 - 同時新增一組登錄值：
 - 登錄名稱：AutoShareServer
 - 登錄類型：DWord
 - 登錄數值：00000000

檢視系統上現有的非預設(自訂增加的)共享資源，請依下列步驟進行：

- 圖形介面（點選我的電腦 - 單擊滑鼠右鍵 - 管理 - 共用資料夾 - 共用）。點選要停用的共享資源 - 單擊滑鼠右鍵 - 選擇「停止共用」。
- 命令列模式（請進入命令提示字元）：
 - 要列舉所有共享資源，請在系統命令提示字元下鍵入指令：

```
net share
```

記下列出的所有共享資源。

- 移除無需使用共享資源，請在系統命令提示字元下鍵入指令：

```
Net share 共享名稱 /delete
```

這只能永久移除非預設(自訂增加的)共享資源，若要移除預設隱藏共享資源 C\$、D\$、ADMIN\$等，請參閱前一節小說明。

- 如果是加入 Windows NT 網域的 Windows 95/98/ME 用戶，請設定用戶級的檔案共用存取控制權限。
- 不要與網際網路的主機共享資源。請確定所有與網際網路界接的主機其 Windows 網路連線控制台上的 Windows 網路共享都已關閉。要與網際網路的主機分享檔案，請透過 SCP、FTP 或 HTTP。
- 不要允許未經身分驗證的分享行為。如果需要分享檔案，就要拒絕任何未經身分驗證的使用者對該分享資源的存取要求。請設定在要求連接分享資源前，對方必需提供密碼。
- 只開放最小需求的共享資源，通常只開放必要的單一資料夾及其子資料夾。
- 只開放對共用資料夾的最小需求權限。特別注意是否需要開啓寫入權限。
- 更甚者，只允許特定 IP 網路位址進入，因為網域(DNS)名稱較容易被偽造。

如何針對匿名登入弱點進行防護

特別注意：本文描述修改共享資源的資訊。在修改共享資源前，請確定如果發生問題時，你知道如何回復這些資源。我們建議對正在運作的主機進行修改前，都要先行測試。想知道與共享資源相關的資訊，請點擊下列文章，看看微軟知識庫中怎麼說：

[256986 - 微軟 Windows 登錄說明](#)

[323170 - 如何備份、編輯和還原 Windows NT 4.0 的登錄](#)

[322755 - 如何備份、編輯和還原 Windows 2000 的登錄](#)

[322756 - 如何在 Windows XP 與 Windows Server 2003 中備份、編輯，以及還原登錄](#)

Windows NT 網域控制站需要使用空連線進行通訊。因此如果使用 Windows NT 網域，或使用 Windows 2000/2003 Active Directory 的混用模式（允許 Windows 2000 之前版本進行存取），則將 RestrictAnonymous 登錄值設為 1 的方式只能限制攻擊者獲取資訊的多寡，而不能完全防止資訊洩露。例如 Security Friday 提供 GetAcct 工具就可以避過 RestrictAnonymous=1 的限制，列舉出 SID 與 UserID。在 Windows 2000/2003 Active Directory 上比較聰明的作法是將 RestrictAnonymous 登錄值設為 2。

要限制空連線所能獲得的資訊，請查閱下列微軟知識庫中的文件：

[143474 - 在 Windows NT 上限制匿名登入使用者獲取資訊](#)

[246261 - 如何使用 Windows 2000 中的 RestrictAnonymous 登錄值](#)

要檢查 RestrictAnonymous 登錄值是否設定有誤，請查閱下列微軟知識庫中的文件：

[296405 - RestrictAnonymous 登錄值可能會破壞 Windows 2000 網域間的信任關係](#)

Windows NT:

1. 開啓登錄編輯器「regedit.exe」，並瀏覽此機碼：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
2. 設定下列登錄值：
登錄名稱：RestrictAnonymous
登錄類型：DWORD 值、數值：1
3. 重新啓動主機。

Windows 2000:

1. 打開「控制台-->系統管理工具-->本機安全性原則」。
2. 打開「本機原則-->安全性原則」。
3. 確定「匿名使用者連線的其他限制」被設定為「沒有明確宣告的匿名權限則不能存取」。
4. 重新啓動主機。

Windows XP:

1. 打開「控制台 -->系統管理工具-->本機安全性原則」。
2. 打開「本機原則-->安全性原則」。
3. 確認啓用下列選項：
4. 網路存取：不允許 SAM 帳號的匿名列舉
5. 網路存取：不允許 SAM 帳號與共用的匿名列舉
6. 重新啓動主機。

如何針對遠端存取登錄值弱點進行防護

要防範此一威脅，請限制對系統登錄值的存取行為，並檢查重要登錄值的存取權限。微軟 Windows NT 4.0 的使用者在進行調整前，必需確認是否已更新 Service Pack 4 (SP4) 以後版本。

特別注意：本文描述修改共享資源的資訊。在修改共享資源前，請確定如果發生問題時，你知道如何回復這些資源。我們建議對正在運作的主機進行修改前，都要先行測試。想知道與共享資源相關的資訊，請點擊下列文章，看看微軟知識庫中怎麼說：

[256986 - 微軟 Windows 登錄說明](#)

[323170 - 如何備份、編輯和還原 Windows NT 4.0 的登錄](#)

[322755 - 如何備份、編輯和還原 Windows 2000 的登錄](#)

[322756 - 如何在 Windows XP 與 Windows Server 2003 中備份、編輯，以及還原登錄](#)

限制網路存取。要限制網路對登錄值的存取，請依下列步驟修改登錄值：

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
- 登錄名稱：Description 類型：REG_SZ
- 登錄數值：Registry Server

此鍵值的安全權限定義了使用者或群組對登錄值的存取權限。在 Windows 預設安裝中定義了此值並在存取控制清單中設定給予本機 Administrator 與 Administrators 群組（及 Windows 2000 中的 Backup Operators 群組）完整存取權限。

修改系統登錄值後，必需重開機才會使它們生效。要限制存取權限，請新增下列登錄值：

Windows 2000 與 NT：

1. 開啓登錄編輯器「regedt32.exe」，並瀏覽此機碼：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
2. 開啓「編輯」選單，點擊「新增機碼」。
3. 輸入機碼名稱：SecurePipeServers，類別：REG_SZ。
4. 瀏覽此機碼：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
5. 開啓「編輯」選單，點擊「新增機碼」。
6. 輸入機碼名稱：winreg，類別：REG_SZ。
7. 瀏覽此機碼：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
8. 開啓「編輯」選單，點擊「新增值」。
9. 輸入值的名稱：Description、資料類型：REG_SZ、字串：Registry Server。
10. 瀏覽此機碼：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
11. 點選「winreg。」，開啓「安全性」選單，點擊「使用權限」，加入要賦與權限的使用者或群組。
12. 退出登錄編輯器，重新啓動微軟 Windows 系統。
13. 如果之後要修改所允許的使用者與群組清單，請重覆步驟 10-12。

Windows XP 與 2003：

1. 開啓登錄編輯器「regedt32.exe」，並瀏覽此機碼：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
2. 開啓「編輯」選單，點擊「新增機碼」。
3. 輸入機碼名稱：SecurePipeServers。
4. 瀏覽此機碼：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
5. 開啓「編輯」選單，點擊「新增機碼」。
6. 輸入機碼名稱：winreg。
7. 瀏覽此機碼：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
8. 開啓「編輯」選單，點擊「新增字串值」。
9. 加入數值名稱：Description、數值資料：Registry Server。
10. 瀏覽此機碼：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
11. 點選「winreg」，開啓「編輯」選單，點擊「使用權限」，加入要賦與權限的使用者或群組。
12. 退出登錄編輯器，重新啓動微軟 Windows 系統。
13. 如果之後要修改所允許的使用者與群組清單，請重覆步驟 10-12。

限制已認可的遠端存取權限。對登錄值進行嚴格限制可能會對相關網路服務造成副作用，像是 Directory Replicator 與網路印表機 Spooler 服務。

爲了避免這些問題，我們可以針對上述權限進行彈性調整，像是將相關服務的執行帳戶加入「winreg」的清單中，或設定 Windows 跳過某些登錄值的存取限制，可在 AllowedPaths 機碼中加上 Machine 或 Users 登錄值：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths
登錄名稱：Machine
登錄類型：多字串值(REG_MULTI_SZ)
預設數值資料：System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Services\Replicator
有效範圍：（可使用的登錄值路徑）
說明：允許主機可存取表列登錄值，除非另有明確限制。

登錄名稱：Users
登錄類型：多字串值
預設數值資料：(無)
有效範圍：（可使用的登錄值路徑）
說明：允許主機可存取表列登錄值，除非另有明確限制。

在 Microsoft Windows 2000 與 Windows XP 登錄值中：

登錄名稱：Machine
登錄類型：多字串值
預設數值資料：System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\control\Server Application System\CurrentControlSet\Services\Eventlog Software\Microsoft\Windows NT\CurrentVersion

登錄名稱：Users (預設不存在)

會這樣作的原因，通常是要因應從弱點公布到修補程式發布之間的時間差距；或因為某些政策考量，這些弱點必需保留。要減低風險，公司組織可透過防火牆或路由器來限制存取行為。另一個方式是撰寫新的 IDS(入侵偵測系統，例如 [Snort](#))偵測規則，可以對相關事件發出警訊，通知各組織進行反應。[Snort](#) 的範例規則可參閱[這裏](#)。

如何針對遠端程序呼叫弱點進行防護

最好的防護方式就是更新 [MBSA](#)、[自動更新功能](#)或 [Windows 更新](#)網站所告知的相關修補程式，請參閱「如何得知你是否具有與遠端程序呼叫相關的弱點」一節的相關說明。如果無法照作，則也有一些方法可以關閉或限制遠端程序呼叫的功能，可由下列網站找到一些不錯的整理：

<http://www.ntbugtraq.com/dcomrpc.asp>

警告：關閉或限制遠端程序呼叫功能可能導致依賴它的 [Windows](#) 服務無法正常運作，請在非運行中的系統環境下先進行變更測試。

如果系統無法進行修補，請由網路邊境阻擋與遠端程序呼叫相關的連接埠(TCP 埠號 135、139、445 與 593，UDP 埠 135、137、138 與 445)。當然，最好的作法還是在網路邊境上預設阻擋「所有」不需使用的服務。

進一步資訊：

[微軟知識庫文件 153183](#)：如何限制從遠端電腦存取登錄。

另一個可參考的資源為 [微軟安全公佈欄線上搜尋服務](#)。

[MSDN 書庫](#)(搜尋「Securing Registry」)。

[微軟知識庫文件 310426](#)：如何使用 [Windows XP](#) 和 [Windows Server 2003](#) 登錄編輯器功能

[網路存取：可遠端存取登錄值路徑與子路徑](#)

[Windows Server 2003 安全手冊](#)

[回頁首 ^](#)

W4. Microsoft SQL Server 資料庫(Microsoft SQL Server, MSSQL)

W4.1 說明

Microsoft SQL Server (MSSQL) 資料庫具有數個安全弱點，可以讓遠端攻擊者獲取機密資訊、修改資料庫內容、佔領 SQL Server，更甚者，在某些設定下還可以佔領主機。

MSSQL 的弱點經常被公開且主動攻擊。最近兩隻 MSSQL 網蟲分別出現在 2002 年五月及 2003 年一月，它們利用的就是數個 MSSQL 的漏洞。被網蟲佔領的主機在掃描其他受害主機時，對網路流量造成極為嚴重的傷害。這些網蟲的進一步資訊可由下列網站找到：

SQLSnake/Spida 網蟲(2002 年五月)

- <http://isc.incidents.org/analysis.html?id=157>
- <http://www.eeye.com/html/Research/Advisories/AL20020522.html>
- http://www.cert.org/incident_notes/IN-2002-04.html

SQL-Slammer/SQL-Hell/Sapphire 網蟲(2003 年一月)

- <http://isc.incidents.org/analysis.html?id=180>
- <http://www.nextgenss.com/advisories/mssql-udp.txt>
- <http://www.eeye.com/html/Research/Flash/AL20030125.html>
- <http://www.cert.org/advisories/CA-2003-04.html>

連接埠 1433 與 1434 (MSSQL 提供服務與監聽的預設埠號)也被網路風暴中心(Internet Storm Centre)視為最常被掃描的埠號。

SQLSnake 的攻擊路徑是利用主機未對預設管理者帳號或「sa」帳號設定密碼。確保所有系統上的系統帳號都具有密碼保護，才是最適當的設定與防護方式；若無，則請完全停用不需使用的帳號。你可以在微軟網路開發文件裏找到〈[變更 SQL Server 管理者登入帳號](#)〉與〈[確認與變更 MSDE 中的系統管理者密碼](#)〉，以管理並設定 sa 帳號的密碼。sa 帳號應該設定一組複雜難猜的密碼，即使你不是使用這個帳號在處理 SQL/MSDE 工作。

SQL Slammer 的攻擊路徑是利用 SQL Server 解析服務(Resolution Service)中的緩衝區溢位弱點。網蟲會送出特製攻擊封包，透過 UDP 埠號 1434 來造成緩衝區溢位以侵入主機。若執行 SQL 服務的主機在收到封包後發生堆疊緩衝區溢位，就會造成伺服器或系統被完全佔領。對抗這支網蟲最有效的方式就是勤於更新、進行系統預防設定、及在網路閘道口過濾對內的 UDP 1434 連接埠的封包。

Microsoft Server 2000 Desktop Engine (MSDE 2000) 可說是一種「SQL Server 簡化版」。許多系統主人甚至不知道在執行 MSDE 時等同於安裝了某個版本的 SQL Server。MSDE 2000 會伴隨下列微軟產品一起安裝：

- SQL/MSDE Server 2000 (Developer、Standard 與 Enterprise 版)
- Visual Studio .NET (Architect、Developer 與 Professional Editions 版)
- ASP.NET Web Matrix 工具
- Office XP
- Access 2002
- Visual Fox Pro 7.0/8.0

除此之外還有許多其他軟體套件都會使用到 MSDE 2000 軟體。可以造訪這個網址以取得最新清單：<http://www.SQLsecurity.com/applicationslistgridall.aspx>。因為這些軟體使用到 MSDE 及其核心資料引擎，所以它們具有與 SQL/MSDE Server 相同的弱點。MSDE 2000 可經由設定接受數種不同方式的客戶端連線。它可以讓客戶端經由 NetBIOS(TCP 埠號 139/445)利用命名管道(named pipes)進行連線，亦可使用 TCP 埠號 1433 的 socket 連線方式，甚至同時並行。無論使用哪一種方式，SQL Server 與 MSDE 都會聆聽 UDP 埠號 1434。客戶端會送訊息到這個埠號，以動態找出它該用哪一種方式與伺服器連結。

當有人對 UDP 埠號 1434 送出單一位元組封包 0x02 時，MSDE 2000 引擎會回傳自身資訊。某些單一位元組封包則可在未經身分驗證的情況下造成伺服器緩衝區溢位。更糟的是，攻擊活動是透過 UDP 管道。無論 MSDE 2000 是以網域使用者還是本機 SYSTEM 帳戶執行，入侵成功都可能讓目標主機被完全佔領。

因為 SQL Slammer 是利用緩衝區溢位來入侵目標系統，所以不斷檢查更新程式與系統設定是降低風險的最佳方式。請下載防護工具來檢查，像是 [Microsoft SQL Critical Update Kit](#) 就可以檢查本機是否具有此弱點、掃描網域或網路中存在的脆弱系統，及自動安裝相關的 SQL 重大更新程式。

請查閱 incidents.org 上的報告與分析來瞭解 SQL/MSDE Slammer 網蟲。2003 年一月 25 日早上，它

在數小時內就影響了網際網路的骨幹。

W4.2 受影響的作業系統：

任何安裝有 Microsoft SQL/MSDE Server 7.0、Microsoft SQL/MSDE Server 2000 或 Microsoft SQL/MSDE Server Desktop Engine 2000，或單獨使用 MSDE 引擎的微軟 Windows 系統。

W4.3 CVE/CAN 項目

[CVE-2000-0202](#), [CVE-2000-0402](#), [CVE-2000-0485](#), [CVE-2000-0603](#), [CVE-2001-0344](#), [CVE-2001-0879](#), [CAN-2002-0649](#)

[CVE-2002-0186](#), [CVE-2002-0187](#), [CAN-2002-0224](#), [CAN-2002-0624](#), [CAN-2002-0641](#), [CVE-2002-0642](#), [CAN-2002-0643](#), [CAN-2002-0644](#), [CAN-2002-0645](#), [CAN-2002-0649](#), [CVE-2002-0650](#), [CAN-2002-0695](#), [CAN-2002-0721](#), [CVE-2002-0729](#), [CVE-2002-0859](#), [CAN-2002-0982](#), [CVE-2002-1123](#), [CVE-2002-1137](#), [CVE-2002-1138](#), [CAN-2002-1145](#), [CAN-2003-0118](#), [Secunia-12680](#)

W4.4 如何得知你是否具有弱點

微軟發布了一系列安全工具，可由此下載 <http://www.microsoft.com/sql/downloads/securitytools.asp>。這個工具包叫作 SQL Critical Update Kit，包含了數個評估工具，像是 SQL Scan、SQL Check 與 SQL Critical Update。

[sqlsecurity.com](#) 的 Chip Andrews 釋出了一個叫作 SQLPingv2.2 的工具。這個工具可以針對單一主機或整個子網送出單一位元組 UDP 封包(值為 0x02)到 UDP 埠號 1434。聆聽 UDP 埠號 1434 的 SQL Server 會回應系統訊息，曝露像是版本號、執行個體(instance)等的系統資訊。SQLPingv2.2 是類似微軟 SQL Scan 的掃描探查工具，並不會進一步危害你的系統或網路安全。其他的 SQL 安全工具亦可在 Chip Andrew 的 [SQL/MSDE 安全網站](#) 上找到。

W4.5 如何針對弱點進行防護

總論：

1. 停用 UDP 埠號 1434 上的 SQL/MSDE 聆聽服務（注意這可能會影響到遠端管理或備份服務）。
2. 套用微軟 SQL/MSDE 伺服器及 MSDE 2000 最新的修補套件。
3. 套用在最新修補套件之後發布的累積更新程式。
4. 套用在最新累積更新程式之後發布的單一更新程式。
5. 啟用 SQL Server 驗證後稽核。
6. 由系統或網路端加強伺服器安全。
7. 給予 MSSQL/MSDEServer 服務及 SQL/MSDE Server Agent 最小權限。
8. 依微軟所提供的最佳實務指示來加強基礎安全。

說明：

1. 停用 UDP 埠號 1434 上的 SQL/MSDE Server 聆聽服務

只要安裝 [SQL Server 2000 Service Pack 3a](#) 並使用內附功能即可達成。微軟資料庫引擎 MSDE 2000 具有兩個緩衝區溢位弱點，可以讓遠端未經身分驗證的攻擊者入侵伺服器。更糟的是，攻擊活動是透過 UDP 管道。無論 MSDE 2000 是以網域使用者還是本機 SYSTEM 帳戶執行，入侵成功都可能讓目標主機被完全佔領。MS-SQL/MSDE Slammer 以極頻繁的速度隨機選取主機，送出一個 376 位元組長的 UDP 封包到它們的 1434 連接埠，被感染的主機也會立刻散播 376 位元組長的封包。這支網蟲會隨機選取 IP 網路位址（包含使用多點傳送協定的 IP 網路位址）送出大量封包，讓目標網路遭到阻絕服務(Denial of service)。據報受害主機被感染後每秒會製造超過 50 Mb 的流量。

2. 套用微軟 SQL/MSDE 伺服器及 MSDE 2000 最新的修補套件。

Microsoft SQL/MSDE Server 最新的修補套件版本為：

- SQL/MSDE Server 7.0 Service Pack 4
- MSDE/SQL Server 2000 Service Pack 3a

想在未來持續追蹤並保持更新，請隨時查詢微軟 TechNet 內的〈[讓你的 SQL/MSDE Servers 不再脆弱](#)〉。

3. 套用在最新修補套件之後發布的累積更新程式。

Microsoft SQL/MSDE Server 最新的累積修補程式為 [MS02-061 SQL/MSDE Server 網頁工作可造成權限提升 \(Q316333/Q327068\)](#)。

想在未來持續追蹤並保持更新，請隨時查詢：

- [Microsoft SQL/MSDE Server 7.0](#)
- [Microsoft SQL Server 2000](#)
- [MSDE Server Desktop Engine 2000 \(MSDE 2000\)](#)

套用在最新累積更新程式之後發布的單一更新程式，並啟用自動更新功能。考慮訂閱微軟安全通知服務(Microsoft Security Notification Service)。在 [MS02-061 SQL/MSDE Server 網頁工作可造成權限提升 \(Q316333/Q327068\)](#) 之後並未發布任何單一更新程式。

4. 啟用 SQL Server 驗證後稽核。

SQL Server 驗證後稽核經常未被啟用。可以使用 Enterprise Manager (選擇伺服器後，在內容屬性下的「安全性」頁籤)。

5. 由系統或網路端加強伺服器安全。

最常被攻擊的 MSSQL/MSDE 弱點，就是預設的管理者帳號(即「sa」)使用安裝時的預設空白密碼。如果 SQL/MSDE 「sa」帳號未受密碼保護，你對於網蟲和攻擊程式是完全沒有抵抗力的。因此，即使你不使用「sa」帳號執行 SQL/MSDE server，你仍然應該依循《[SQL Server 線上叢書](#)》內〈系統管理員(sa)登入〉一節中的建議來確保內建的「sa」帳號具有強韌密碼。MSDN 也有兩份文件：〈[變更 SQL Server 管理者帳戶](#)〉與〈[如何驗證與變更 MSDE 系統管理員密碼](#)〉。

6. 給予 MSSQL/MSDEServer 服務及 SQL/MSDE Server Agent 最小權限。

使用具有最小權限的合法網域帳號來執行 MSSQL/MSDEServer 服務與 SQL/MSDE Server Agent，不要使用網域管理者或 SYSTEM(NT 平台)或 LocalSystem (2000 或 XP 平台)帳號。具有本機或網域權限的服務一旦被佔領，可以讓攻擊者取得主機或整個網路的控制權。

- a. 啟用 Windows NT 認證模式，啟用對登入成功與失敗的安全稽核，再重新啟動 MSSQL/MSDEServer 服務。如果可以的話，也將客戶端設定使用 NT Authentication 認證模式。
- b. 網路邊境上應使用封包過濾機制，以禁絕 MSSQL 服務上未經授權對內或對外的連線。過濾 TCP/UDP 埠號 1433 與 1434 的封包可防止內部與外部攻擊者進行掃描，或侵害具有弱點的微軟 SQL/MSDE 伺服器，也可禁絕內部或其他網路上未經授權而公開提供的 SQL/MSDE 服務。
- c. 如果網際網路閘道上必需允許使用 TCP/UDP 埠號 1433 與 1434，請自行修訂過濾規則來防止這些埠號被誤用。

關於加強微軟 SQL/MSDE Server 安全性的進一步資訊，可參閱：

- [微軟 SQL/MSDE Server 7.0 安全](#)
- [微軟 SQL/MSDE Server 2000 安全](#)

[回頁首 ^](#)

W5. Windows 身分驗證(Windows Authentication)

W5.1 說明

使用者與資訊系統間的每次交談幾乎都會用上密碼字串、密碼短語或安全驗證碼。多數的使用者認證形式、檔案及資料的保護機制都是依靠使用者密碼。驗證成功所進行的存取行為通常未加記錄，這樣的記錄也不容易讓人生疑，因此密碼洩露就成了一种難以被系統察覺的攻擊。攻擊者有權存取具有受害者權限的所有資源，甚至可以存取其他帳號、鄰近主機或管理者權限。儘管有這種安全威脅，使用脆弱密碼或空白密碼的例子仍然極為常見，有訂立密碼安全政策的組織更是少之又少。

常見的密碼弱點有：

- 使用者使用脆弱密碼或無密碼。
- 雖然密碼強度夠，但是使用者未加以妥善保護。
- 作業系統或第三方應用程式會新增具有脆弱密碼或無密碼的帳號。
- 多數商業或開放原始碼的應用程式都使用公開的雜湊演算法(hashing algorithm)，而密碼雜湊值(hash)儲存於一般使用者均可存取的地方。若系統政策無法保護雜湊演算法實作時所造成的弱點時，則使用強韌密碼可以讓雜湊值較難被還原回原始密碼。

微軟 Windows 並不使用明文儲存或傳送密碼，它使用密碼雜湊值進行驗證。雜湊值是由一個數學函數(雜湊演算法)將任意長度資料進行運算後，所產生出來的固定長度資料，又被稱為訊息摘要。Windows 驗證演算法有三種：LM (最不安全、但較為通用)、NTLM 與 NTLMv2 (最安全，但較不通用)。雖然大多數 Windows 環境都不需要 LAN Manager (LM)，Windows NT、2000 與 XP 仍會預設將傳統的 LM 密碼雜湊值儲存於本機(又被稱為 LANMAN 雜湊值)，Windows 2003 已經取消這項設定。因為 LM 使用的加密方式遠較微軟現行其他演算法(NTLM 與 NTLMv2)為弱，有心者可在短時間內破解 LM 密碼。即使使用強韌密碼，今日的硬體仍可用暴力猜解法在一週內解出。

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/h_gly.asp

LM 雜湊值脆弱的原因如下：

- 密碼只有前 14 字元有效
- 不足 14 字元的密碼，會使用空白字元補到 14。
- 密碼被強迫轉換成大寫字母儲存。
- 密碼被分割為兩個 7 字元長的部分。

這種雜湊實作方式代表了攻擊者只要針對兩組 7 個字元長、全大寫字母密碼進行破解，即可通過驗證取得主機存取權限。因為破解雜湊值的複雜程度與雜湊值長度成幾何正比，暴力破解 7 字元長的字串可比破解 14 位元長的字串簡易上許多。而又因為這 7 個字元(還包含空白字元)都是大寫字母，利用字典攻擊時也可以省下許時間。如果密碼長度不足 14 字元，LM 雜湊值會補上空白直到 14 字元長，亦即分開後第二段密碼真正長度不足 7 字元。因此使用超過 14 字元的密碼，才可以稍微增加暴力猜解的難度。注意，上述問題不只發生在 Windows 環境，只要可以取得密碼雜湊值，就有被攻擊者進行暴力猜解的潛在風險。

LM 雜湊值還被儲存在 SAM 中，用戶端會預設使用 LAN Manager 進行驗證，而伺服器也預設接

受。造成的結果是即使 Windows 主機用了較強的雜湊演算法，還是會將脆弱的 LM 雜湊值送到網路上。Windows 驗證過程中若遭到封包測錄 竊聽，攻擊者仍可輕易取得使用者密碼。

W5.2 受影響的作業系統：

所有微軟 Windows 作業系統

W5.3 CVE/CAN 項目

[CVE-2000-0222](#)

[CAN-1999-0504](#), [CAN-1999-0505](#), [CAN-1999-0506](#)

W5.4 如何得知你是否具有弱點

因為密碼弱點而造成的威脅多半具有明顯特徵，像是離職員工帳號若還在進行活動就很容易被注意到。但要在事前確認每個密碼是否夠強韌，唯一的方法就是跟攻擊者使用同一套工具來進行測試。

注意：若無長官允許，絕對不要使用任何密碼破解器，即使是針對你有管理權限的系統。許多好心的管理者因為未經授權執行密碼破解器而被開除。

最好的幾個破解工具如下：[LC6 \(L0phtcrack 第 5 版\)](#)及 [John the Ripper](#)。

關於本機儲存 LAN Manager 雜湊值的問題：

- 如果你是用 NT、2000 或 XP 的預設安裝，你就具有本機儲存 LAN Manager 雜湊值的弱點，不過預設只有系統管理者具有存取權限。
- 如果你的工作環境中有需要使用 LM 驗證的傳統伺服器，則你就具有此弱點，因為網路上傳送 LM 雜湊值可能會被竊聽。

W5.5 如何針對弱點進行防護

預防密碼弱點的最佳方式是制定好的安全政策，教導使用者養成良好的密碼習慣，並事先檢查密碼的完整性。

- **確認密碼夠強韌。**只要硬體夠好、時間足夠，任何密碼都可被暴力猜測破解。甚至還有一些更簡易的方法，密碼破解器使用的一種方式稱作字典攻擊法(Dictionary attack)。因為雜湊演算法是公開的，破解工具只要將所獲得的雜湊值與字典單字(可由各種語言中選取)所產生的雜湊值相比對，即可猜出原始密碼。所比對的單字還可與名字組合，或重新排列以擴展選擇範圍。用已知單字而造出的密碼是很容易被猜解出來的。許多組織都規定使用者密碼除了純字母之外，還要混用特殊符號，因此許多使用者就將原來的單字密碼(password)的部分字元用特殊符號取代(pas\$\$wOrd)。雖然這種轉換可以防止字典攻擊，但遇上以所有可列印字元為破解目標的攻擊方式仍是難以抵抗。

好的密碼來源不該包含單字或名字。強韌的密碼政策應該告訴使用者用更隨機的方式來選擇密碼素材，像是一句話、書名或歌名。使用者可藉著將句子連結成長字串(像是將每個單字的第一個字母連在一起、或取代單字中的某些字母、移除所有母音等)，而造出一個夠長，且包含純字母與特殊字元的密碼，讓字典攻擊法難以破解。如果原本的句子很難忘記，則轉換出來的密碼也一樣刻骨銘心。

一旦制定了密碼產生規則，安全政策就要落實以確保使用者遵循這個流程。最好的方式就是在使用者變更密碼時就使用 Passfilt (NT4)來進行檢查。

Windows 2000、XP、2003 上都有強制規定密碼政策的工具。要檢視 Windows 系統上現行

的密碼政策，請依下列步驟進行：開始 – 設定 – 控制台 – 系統管理工具 – 本機安全性原則 – 選擇帳戶原則 – 密碼原則。本機安全性原則具有以下設定：

- **密碼必須符合複雜性需求。**決定密碼必須符合複雜性需求。建立或變更密碼時會強制執行複雜性需求。如果啓用了此原則，則密碼必須符合下列最小需求：
 - 不含全部或部分使用者帳戶名稱
 - 長度至少為 6 個字元
 - 包含下列四種字元中的三種：
 - 英文大寫字元 (A 到 Z)
 - 英文小寫字元 (a 到 z)
 - 10 個基本數字 (0 到 9)
 - 非英數字元 (如 !、\$、#、%)
- **強制執行密碼歷程記錄 (0-24 個)：**決定重覆使用舊密碼前需經歷過的不同新密碼數目。此值必須介於 0 和 24 個密碼之間。將此參數設為記憶 0 個密碼代表密碼可被重覆利用，設為記憶 24 個密碼則代表需使用 24 個不同密碼後才可重覆使用最初的密碼。這個原則可讓系統管理員藉由確認舊密碼不再被繼續使用來增加安全性。為維護密碼歷程記錄的有效性，在設定密碼有效期限時，請拒絕立即變更密碼。
- **密碼最長有效期 (0-999 天)：**指定系統要求使用者變更密碼之前，密碼可以使用的期限 (天數)。您可以設定密碼在 1 和 999 之間的天數後到期，或是設定天數為 0，藉以指定密碼永遠不會到期。
- **密碼最短有效期 (0-999 天)：**指定使用者變更密碼之前，密碼必須使用的期限 (天數)。您可以設定 1 和 999 天之間的值，或設定天數為 0，以允許立即變更。密碼最短有效期必須小於密碼最長有效期。如果您要強制執行密碼歷程記錄生效，請將密碼最短有效期限設為 0 以上。若沒有設定密碼最短有效期限，使用者便可重覆使用密碼，直到厭倦為止。預設值並未遵循此建議，所以系統管理員可為使用者指定密碼，然後在使用者登入時要求變更系統管理員定義的密碼。如果密碼歷程記錄設為 0，使用者便不需要選擇新密碼。因此，密碼歷程記錄預設為 1。
- **最小密碼長度 (0-14 字元)：**決定使用者密碼可包含的最少字元數。您可以設定介於 1 和 14 個字元之間的值，或設定字元數為 0，如此便不需要密碼。最小密碼長度必需符合公司的安全政策(若無相關安全政策，則建議設為 8 以上。[美國國家安全局](#) 建議使用 12 個字元)。
- **使用可復原的加密儲存網域中所有使用者的密碼：**決定 Windows 2000 Server、Windows 2000、2003 以及 Windows XP Professional 是否使用可復原的加密來存放密碼。此原則支援應用程式使用需要知道使用者密碼來進行驗證的通訊協定。使用可復原的加密來存放密碼，基本上和存放純文字密碼是相同的。基於這個理由，除非應用程式需求比保護密碼資訊重要，否則絕不應該啓用這個原則。

有個方法可用來為使用者自動產生複雜性密碼，請由 Windows NT4、2000、XP、2003 的命令提示字元下執行下列命令：

```
net user 使用者名稱/random
```

執行此命令會將為目標帳戶設定一組隨機密碼(但固定為 8 位元長)，並將密碼列印於螢幕上。通常適合使用於服務程式帳戶上，而非一般使用者。

稽核密碼品質的最好方法，是在定期掃描時同步獨立執行密碼破解工具。

特別注意：若無長官允許，絕對不要使用任何密碼破解器，即使是針對你有管理權限的系統。許多好心的管理者因為未經授權執行密碼破解器而被開除。

一旦你獲得執行密碼破解器的許可，請定時在安全的獨立主機上執行。秘密通知密碼被破解成功的

使用者，同時告知選擇良好密碼的方式。系統管理員與公司管理者必需合作研擬相關流程，以便在使用者不肯合作時，請公司管理者出馬協助。

另一種防止未設密碼或脆弱密碼的方法就是改用其他驗證方式，像是密碼生成憑證或生物辨識。

1. **保護強韌密碼。**即使密碼夠強韌，使用者若不好好保管密碼，帳號還是會被盜用。良好的安全政策應該告訴使用者千萬別隨便透露密碼、不要將密碼寫在別人看得到的地方、並保護好自動驗證時會儲存的密碼檔案(例如開啓自動登入功能，最好的保護方式就是避免這類設定，只有在需要時才鍵入密碼)。落實密碼有效期的政策，不要使用舊密碼，即使密碼外洩，也只有短期間能造成影響。在密碼到期前就該警告使用者，並請他們更改密碼，因為使用者在突然看到「你的密碼已到期，必須馬上進行更改。」訊息時，通常會傾向選擇簡單好記的密碼。
2. **防止密碼雜湊值與 SAM 資料庫被複製。**在前一節提到過密碼破解器，它們的破解素材為：
 - 由網路上竊聽密碼。
反制方式：1.使用交換式網路；2.偵測並移除網路上使用雜亂模式(promiscuous mode)的網路卡(大多數商用安全評估軟體都可以偵測到，例如免費工具 [ethereal](#))。
 - 複製出 SAM 檔案(位於%SystemRoot%\System32\Config\資料夾，在 Windows NT4 與 2000 下通常在 C:\Winnt\System32\Config\，Windows XP 與 2003 下通常在 C:\Windows\System32\Config)。這個檔案在正常情形下會被 Windows 作業系統鎖定，只能在使用另一個作業系統開機時才能複製出。但可在備份回復 SAM 檔或系統狀態下取出(Windows 2000, 2003, XP)。SAM 檔亦位於 NT4 救援磁片上。
反制方式：限制或監看主機(特別是網域控制站)、備份媒體與救援磁片的實體存取權限。

微軟提供了一些有用的參考文件：
 - [〈如何在 Windows NT 上停用 LM 驗證〉 \[Q147706\]](#) 詳述了如何在 Windows 9x 與 Windows /NT/2000 下變更登錄值。
 - [MS03-034：NetBIOS 中的瑕疵可能會導致資訊洩露 \(824105\)](#)
 - [〈LMCompatibilityLevel 及它的功用〉 \[Q175641\]](#) 解釋了這個參數的內部運作方式。
 - [〈如何為 Windows 95/98/2000/NT 啓用 NTLMv2 身分驗證〉 \[Q239869\]](#) 解釋了如何使用 Windows 2000 的目錄服務用戶端程式為 Windows 95/98 克服 NTLMv2 相容性問題。[〈用來將 LM 雜湊從 Active Directory 及安全性帳戶管理員中移除的新登錄機碼〉](#)
3. **嚴格控管帳號。**
 - 任何未使用的服務程式帳號或管理帳號應被停用或移除。任何使用中的服務程式帳號或管理帳號應更新成強韌密碼。
 - 定期稽核所有系統上的帳號，並列出一份所有帳號的管理清單。不要忘記檢查路由器、網路數位印表機、影印機和印表機連接器等系統上的密碼。
 - 訂立作業流程以將認可帳號加入清單、並移除不使用的帳號。
 - 定期檢查清單是否需加入新帳號或移除舊帳號。
 - 員工或合約人離職，且帳號不再需要時，一定要有相關流程以確實移除其帳號。
4. **維護公司的強韌密碼政策。**除了由作業系統或網路面控制外，還有很多全面性的工具可以幫助管理良好的密碼政策。你可以在 [SANS 安全政策專案](#) 網站中找到許多範例政策範本、政策制訂準則、密碼安全基礎及各安全政策網站(含密碼政策訊息)的連結。
5. **停用 LM 的網路驗證。**Windows 下替換 LAN Manager 驗證模式的最佳方案是 NT LAN Manager 第二版 (NTLMv2)。NTLMv2 挑戰與回應模式利用強加密及改良後的身分驗證與工作階段安全機制，克服了許多 LM 的弱點。Windows NT 與 2000 下設定這項功能的登錄

值都在：

登錄群：HKEY_LOCAL_MACHINE
登錄機碼：System\CurrentControlSet\Control\LSA
登錄名稱：lmcompatibilitylevel
登錄類型：REG_DWORD
有效範圍：0-5
預設值：0

說明：此參數決定要使用哪種驗證模式。

- 0 - 傳送 LM 和 NTLM 回應，絕不使用 NTLMv2 工作階段安全。
- 1 - 傳送 LM 和 NTLM，如有交涉，使用 NTLMv2 工作階段安全性。
- 2 - 只傳送 NTLM 回應。
- 3 - 只傳送 NTLMv2 回應。
- 4 - 網域控制站只傳送 NTLMv2 回應\拒絕 LM。
- 5 - 網域控制站只傳送 NTLMv2 回應\拒絕 LM 和 NTLM。

在 Windows 2000、2003 與 XP 上，可啓用「LAN Manager 驗證層級」(Windows 2000)或「網路安全性：LAN Manager 驗證層級」(Windows XP, 2003)（開始 – 設定 – 控制台 – 系統管理工具 – 本機安全性原則 – 選擇本機原則 – 安全性選項）。

如果所有系統都已更新至 Windows NT SP4 之後，你可將所有用戶端設為 3、所有網域控制站設為 5 以杜絕在網路上傳送 LM 雜湊值。然而舊版系統(像是 Windows 98/98)預設的微軟網路用戶端程式無法使用 NTLMv2。要相容 NTLMv2，請安裝目錄服務用戶端程式。安裝後，「LMCompatibility」登錄值就允許被設為 0 或 3。

如果無法強迫舊版系統的用戶端使用 NTLMv2，你也可藉由強迫使用 NTLM (NT Lan Manager 第一版) 來提升一點點安全性。請將網域控制站上的 LMCompatibilityLevel 值設為 4，或使用「本機安全性原則」將「LAN Manager 驗證層級」設為「只傳送 NTLMv2 回應\拒絕 LM」。但最安全的方法是將舊版系統轉換為新版系統，因為舊版作業系統無法指定最小安全層級。

6. **避免儲存 LM 雜湊值。** 單單只是不讓 LM 雜湊值在網路上傳輸，仍然不能阻止它們被產生並儲存於 SAM 或 Active Directory。微軟有一套機制可以關閉 LM 雜湊值的產生功能，但只能使用於 Windows 2000、2003 與 XP。在 Windows 2000 系統 (SP2 之後版本)，下列登錄值控制了這個函數：

登錄群：HKEY_LOCAL_MACHINE
登錄值：System\CurrentControlSet\Control\LSA\NoLMHash

如果是在 Windows 2000 網域控制站增加這個登錄值，則 LanMan 雜湊值就不會被產生且儲存於 Active Directory。

在 Windows XP 與 2003 上，可啓用「網路安全性：下次變更密碼時不儲存 Lan Manager 雜湊次數值」（開始 – 控制台 – 系統管理工具 – 本機安全性原則 – 選擇本機原則 – 安全性選項）。

在進行上述修改後，Windows 2000 系統必需重新啓動，這些設定才會生效。

特別注意： 這只預防產生新的 LM 雜湊值。現存的 LM 雜湊值只會在每個使用者下次個別修改密碼時被移除。

W6. 網頁瀏覽器(Web Browsers)

W6.1 說明

瀏覽器是微軟 Windows 系統上的電腦使用者存取網頁的工具。使用者最多的瀏覽器是 Microsoft Internet Explorer (IE)，這是微軟 Windows 平台預設安裝的網頁瀏覽器。其他的網頁瀏覽器還包含了 Mozilla、Firefox、Netscape 與 Opera。IE 最新版本為 6，[US-CERT](#) 曾發布一個通告來描述 IE 6 在安全方面的改進與功能。以下提到的弱點也同樣影響到 Mozilla 1.4 版-1.7.1 版、Firefox 0.9.x 版、Netscape 7.x 版與 Opera 7.x 版。

這個問題分為六大項：

1. 過去幾年發現的弱點數目遠遠超過其他瀏覽器 – 依 [Security Focus 資料倉庫](#) 記載，2001 年四月之後至少發現了 153 個 IE 弱點。
2. 對已知的 IE 弱點的修補時間過長 – 在弱點被公布後，使用者等了六個月以上微軟才發布修補程式
3. Active X 和 Active Scripting 控制項本身並未發現特定的公開攻擊程式，但可被用於避過瀏覽器安全架構，對主機造成潛在影響。
4. 大量的未修補弱點 – <http://umbrella.name/computer/originalvuln/msie/> 公布了至少 34 個。
5. 間諜軟體/廣告軟體弱點 – 這影響到所有瀏覽器及協助存取網頁的系統
6. 將 IE 瀏覽器整合在作業系統中，使得作業系統更容易被入侵。

所有的網頁瀏覽器與應用程式都有自己的安全弱點或程式問題。惡意的網頁設計者可以撰寫特製網頁，讓瀏覽者在瀏覽時發生程式錯誤而被入侵。最著名的範例為「[Download.Ject](#)」弱點，已在網路上橫行好幾個月了，它使用的是 Active X 弱點。即使 2004 年 6 月 8 日即有攻擊程式公布，IE 的相關修補程式直到七月還沒出現。因為 Microsoft Internet Explorer 被產業與家庭使用者廣為使用，它也成了攻擊者最感興趣的目標。然而最大的風險才剛出現，像是跨站腳本程式碼攻擊(cross-site-scripting, XSS)就是以瀏覽器為主要目標的惡意手法。其他瀏覽器攻擊法包含了 cookie、本機檔案或資料造成的資訊洩露、下載並執行任意程式碼、或完全掌控受害系統等。

W6.2 受影響的作業系統：

這些弱點存在於任何執行上述瀏覽器的微軟 Windows 系統。要注意的是，大多數微軟軟體都預設安裝 IE，即使使用者不想安裝或使用，它通常都還是會存在於你的 Windows 系統。其他瀏覽器都是由使用者自行安裝，使用者也可以決定其他應用程式是否需要用到瀏覽器。

W6.3 瀏覽器弱點，由 [Secunia](#) 提供

會有重覆，因為某些弱點存在於所有瀏覽器上

A. Internet Explorer 弱點：

2004 - 15 則安全通報 (至 2004 年 7 月 30 日止)

1. [Microsoft Internet Explorer 多項弱點](#)
2. [Internet Explorer 框架注入弱點](#)
3. [Internet Explorer 下載檔案的錯誤訊息造成阻絕服務](#)
4. [Internet Explorer 可迴避安全性區域並假造網址列](#)
5. [Internet Explorer 本機資源存取及跨區域腳本程式碼弱點](#)
6. [微軟 Internet Explorer 及 Outlook URL 欺騙法](#)
7. [Windows Explorer / Internet Explorer 分享檔名過長導致緩衝區溢位](#)
8. [Microsoft Outlook Express MHTML URL 處理弱點](#)
9. [Internet Explorer/Outlook Express 「限制的網站」狀態列可被假造](#)
10. [多種瀏覽器 Cookie 路徑跳脫弱點](#)

11. [Internet Explorer 迴避跨框架腳本程式限制](#)
 12. [Internet Explorer 辨識本機檔案](#)
 13. [Internet Explorer 瀏覽記錄可被植入腳本執行程式](#)
 14. [Internet Explorer 下載檔案可假造副檔名](#)
 15. [Internet Explorer 迴避 showHelp\(\) 限制](#)
- B. Mozilla 弱點：
- 2004 - 7 則 Secunia 通報
1. [Mozilla 無法限制對"shell:"的存取](#)
 2. [Mozilla XPInstall 對話方塊安全問題](#)
 3. [多種瀏覽器框架注入弱點](#)
 4. [Mozilla 瀏覽器可被假造網址列](#)
 5. [Mozilla / NSS S/MIME 實作弱點](#)
 6. [多種瀏覽器 Cookie 路徑跳脫弱點](#)
 7. [Mozilla 跨站腳本程式碼攻擊](#)
- C. Netscape 弱點：
- 2004 - 2 則 Secunia 安全通報
1. [Mozilla 未限制對"shell:"的存取](#)
 2. [多種瀏覽器框架注入弱點](#)
- D. Opera 弱點：
- 2004 - 8 則 Secunia 安全通報
1. [Opera 瀏覽器可被假造網址列](#)
 2. [多種瀏覽器框架注入弱點](#)
 3. [Opera 假造網址列安全問題](#)
 4. [Opera 瀏覽器可透過 Favicon 顯示假造網址列](#)
 5. [多種瀏覽器 Telnet 協定處理器可操縱檔案](#)
 6. [Opera 瀏覽器可被假造網址列](#)
 7. [多種瀏覽器 Cookie 路徑跳脫弱點](#)
 8. [Opera Browser 下載檔案可假造副檔名](#)

W6.4 找出瀏覽器弱點並加以保護

如果你的系統使用 Internet Explorer，目前並沒有方法確定是否有弱點，因為許多弱點尚未被修補。應定時造訪 [Windows 更新網站](#)。可能的話，啓用 [自動更新](#) 功能，確報最新的弱點能夠被即時修補以保護 IE。想進一步了解瀏覽器弱點的使用者，可依下列建議：

- a. 要擁有最安全的瀏覽環境，要有效的方法就是讓網頁瀏覽器的版本保持最新，以獲得新的控制功能、提升安全性並清除已知的舊版問題。舉例而言，最新版的 IE 可由此免費下載：<http://www.microsoft.com/windows/ie/>
- b. 大多數網站不使用 Active X，但停用此功能可能會對系統造成其他問題。例如使用 Active X 的 [Windows 更新網站](#) 就會受影響。你可以試著使用 [自動更新](#) 功能代替。其他的更新選擇還包含了使用 [Shavlik 的 HFNetChkPro™](#) 或 [Microsoft Baseline Security Analyzer \(MBSA\)](#)，皆可達到相同目的。而像是 [Qualys Browser Check](#) 之類的線上 Internet Explorer 分析工具對於評估系統上的 IE 狀態是十分有幫助的。
- c. 平時應遵循「最佳用法」中的指示，在使用管理者帳號登入，或具有高系統權限時，不要瀏覽網頁或存取網頁資源。
- d. 如果無法換用其他瀏覽器，請考慮除了可內部所需使用的 ActiveX applet 外，停用所有 ActiveX 項目；ActiveX applet 可預先安裝於系統內。微軟提供了一個使用 Internet Explorer 來停用 Active 控制項的方法，這些控制項在 Windows XP SP2 後也增強了安全性。

其他瀏覽器並不像 Internet Explorer 具有自動工具。如果你使用 Mozilla/Firefox、Netscape 或 Opera，你應該隨時檢視相關網站 (<http://www.mozilla.org>、<http://www.netscape.com>、<http://www.opera.com>) 或 <http://umbrella.name>) 來追蹤弱點與修補方式。

W6.5 如何保護 Internet Explorer 安全

要設定 Internet Explorer 的安全性前，請先確定作業系統已套用最新的服務套件與更新程式。在 Windows XP 上就要安裝 [Service Pack 2](#)：

1. 從「工具」選單中選擇「網際網路選項」。
2. 選擇「安全性」頁籤，在「網際網路」區域中點擊「自訂層級」。

多數的 IE 弱點都是透過 Active Scripting 或 ActiveX 控制項。

3. 在「指令碼處理」下方選擇將「允許透過指令碼執行貼上動作」設為「停用」，以避免剪貼簿內容造成危害。

註： 停用 Active Scripting 可能會造成某些網站無法正常瀏覽。

ActiveX 控制項雖不常用，但因為它有極大系統權限而具有潛在危險。請到「Active X 控制項與插件」下：

4. 選擇停用「下載簽名的 Active X 控制項」。
5. 選擇停用「下載未簽署的 Active X 控制項」。
6. 同時選擇停用「起始不標明為安全的 Active X 控制項」。

Java applets 具有比一般腳本程式更多的能力。因此在進行系統操作或維護時，最好還是不要使用管理者權限。

7. 在「Microsoft VM」下將「Java 權限」設定為「高度安全」，以確保 Java applet 被限制在 sandbox 下執行，避免它取得權限存取你的系統。
8. 在「雜項」下選擇停用「存取各網域的資料來源」以幫助避過跨網站腳本程式碼攻擊。

也請確定「信任的網站」與「近端內部網路」兩個區域中沒有未受信任的網站，因為這兩個區域的安全性比其他區域來得弱。

[回頁首 ^](#)

W7. 檔案共享應用程式(File-Sharing Applications)

W7.1 說明

使用點對點檔案共享程式 (P2P) 的使用者與日俱增。這些應用程式是用來下載並散布各種型態的資料(像是音樂、圖片、文字、原始碼及一些專利資訊上所列出的資料類別)。P2P 應用程式有不少正當用途，包含散布開放式原始碼/GPL 程式、Linux 系統開機光碟的 ISO 映像檔、獨立藝人的創作、甚至商用媒體的電影預告、遊戲試玩版等。但在其他情況下，資料是否具有版權就值得深究了。依 Napster 法律訴訟事件可知，P2P 程式的主要運作方式為透過分散的網路用戶端來分享檔案目錄或整個硬碟。使用者可以在用戶端軟體上鍵入要搜尋的檔案與參數，參加者之間就會建立起多個通訊管道，讓程式尋找哪個網路用戶擁有所需的檔案。使用者藉由同時下載與分享檔案來加入點對點的分享世界，在某些模式下，上層還有專門負責在多使用者間進行搜尋的節點。

點對點通訊中包含了索取檔案的要求、回應及檔案傳輸。參加者可以在要求下載多個檔案的同時，也提供多個檔案的上傳。搜尋字串可使用使用者能想到的任何文字。大多數軟體都使用預設埠號，但是為了應付網路偵測、防火牆或是封包過濾器，也可以自動或手動調到不同埠號。搜尋與傳輸活

動的多執行緒特性在密集的区域網路上會造成明顯的網路流量，使網路完全充斥了對廣域網路的連線。

P2P 軟體具有不少弱點，約可分成三類。技術上的弱點可讓它們被遠端入侵，社交上的弱點則是將篡改或隱匿後的二進位檔案上傳給要求者，法律上的弱點代表那些侵害版權或讓一般人心生厭惡的資料內容。

如上所述，技術上的弱點可被遠端入侵，或發生在使用者下載、安裝、執行抓回的程式時。下面的 CVE 與 CAN 項目都是在討論技術上的弱點。影響層面從可能造成阻絕服務，到可讓人存取任意檔案，因此不得不慎重待之。P2P 程式還可能會洩露機密或隱私，雖然這並未列入 CVE 資料庫，但仍是很嚴重的安全問題。許多這類應用程式都含有間諜軟體或廣告軟體元件，在將使用者的網路瀏覽習慣回報給程式作者時，也佔用了極大的網路頻寬。設定不良的 P2P 用戶端程式可能因為分享了整個硬碟，而讓網路上所有人都可不經身分驗證直接存取。幾乎沒有任何方式可以限制共享的檔案型態，因而最後常常導致機密資訊、智慧財產權與其他資料外洩。

社交弱點的存在，通常因為惡意或已受感染的使用者新增或變更有問題的檔案提供其他使用者下載。病毒、木馬程式、網蟲和其他惡意程式都是這類產物。受害者通常是非技術人員，他們通常不會注意檔案或圖示的副檔名以及真正關聯型態，而直接點擊開啓檔案，因而被騙執行了惡意程式。無論所下載的檔案內容為何，使用者都應使用最新的防毒軟體進行掃描，並儘可能比對檔案的檢查碼，以確保所下載的檔案是使用者所需、也是檔案作者原始提供的。P2P 機制也常被來散布惡意程式，許多病毒藉由藏在 P2P 內容檔案中來擴散，一旦感染目標，就將自己儲存到感染者的分享資料夾下。P2P 的網路流量也可拿來掩護對跳板主機(又稱為殭屍)的控制與命令封包。

無論是公司或是個人都必需正視法律上的弱點。透過 P2P 程式取得的內容包含了版權音樂、電影與程式檔案。MPAA、RIAA 與 BSA 等組織都虎視眈眈地想終止 P2P 網路侵害版權的行為，在美國隨處可見針對使用者代號寄出的法院傳票、禁止令和民事訴訟。但是這些行動是否有效、哪裏不足、下載檔案是否道德等議題，跟公司必需上法庭辯護的成本比起來都是微不足道。色情圖片同樣也在 P2P 網路上泛濫。當你們公司有員工用公司電腦下載這類資料，讓另一位員工覺得受冒犯而對公司提起騷擾訴訟時，這種內容就算在公司所在轄區內合法也無濟於事了。

W7.2 受影響的作業系統：

Windows 作業系統上現有許多各版本的 P2P 軟體，UNIX 與 Linux 系統亦同。

W7.3 CVE/CAN 項目

[CAN-2000-0412](#), [CVE-2001-0368](#), [CAN-2002-0314](#), [CAN-2002-0315](#), [CVE-2002-0967](#), [CAN-2003-0397](#)

W7.4 如何得知你是否具有弱點

偵測網路上的 P2P 活動著實是項挑戰。你可以藉由監控 P2P 軟體常用埠號的網路流量，或找尋 P2P 軟體常用的某些應用層字串來偵測是否有人使用 P2P 軟體。請參考下面所列的 P2P 常用埠號。有不少應用與服務程式可協助偵測或預防 P2P 網路活動。某些主機型入侵防禦軟體還可以防止安裝或執行 P2P 程式。Cisco 的網路端應用層辨識儀(NBAR)和其他網路端產品都可監控並預防 P2P 封包的進出。利用 NTOP 之類程式來監控你的廣域網路連線也可以找出 P2P 的網路流量。你也可以在網路儲存節點上掃描是否有使用者最常下載的檔案類型，包含*.mp3、*.wma、*.avi、*.mpg、*.mpeg、*.jpg、*.gif、*.zip、*.torrent 與*.exe。監控磁碟殘餘空間是否突然減少也是種方法。Nessus 有一些插件可以偵測是否有執行 P2P 程式，SMS 可掃描微軟 Windows 主機來找出工作主機上安裝了哪些程式。

W7.5 如何針對弱點進行防護

公司政策：

1. 公司必需針對下載 版權軟體與資料的行為制定政策並落實。
2. 公司必需針對公司網路使用方式制定可接受的政策並落實。
3. 定期掃描網路儲存節點及公司的工作主機，尋找是否有未經授權的資料。

網路限制：

1. 一般使用者不應具有安裝軟體的權利，尤其是點對點程式。
2. 考慮使用代理伺服器來控制網路存取狀況。
3. 對外封包的過濾規則對非公司所需的埠號連線必需嚴格限制，但因為許多 P2P 程式都已換用 http 的埠號，這個防護方式較沒有效用。
4. 監控網路上的 P2P 流量，透過相應管道找出違反政策的行為。
5. 布署企業級的防毒軟體，每天更新病毒碼。

點對點應用程式的常用埠號

Napster	eDonkey	Gnutella	KaZaa
tcp 8888	tcp 4661	tcp/udp 6345	tcp 80 (WWW)
tcp 8875	tcp 4662	tcp/udp 6346	tcp/udp 1214
tcp 6699	udp 4665	tcp/udp 6347	
		tcp/udp 6348	

Snort 偵測特徵資料庫中的相關項目：<http://www.snort.org/cgi-bin/sigs-search.cgi?sid=p2p>

ID	項目
549	P2P napster 登入
550	P2P napster 新使用者登入
551	P2P napster 要求下載
552	P2P napster 要求上載
556	P2P 對外的 GNUTella 用戶端要求
557	P2P GNUTella 用戶端要求
559	P2P 對內的 GNUTella 用戶端要求
561	P2P Napster 用戶端資料
562	P2P Napster 用戶端資料
563	P2P Napster 用戶端資料
565	P2P Napster 伺服器登入
1383	P2P Fastrack (kazaa/morpheus) 索取要求
1432	P2P GNUTella 索取
1699	P2P Fastrack (kazaa/morpheus) 流量
2180	P2P BitTorrent 通知要求
565	P2P Napster 伺服器登入
2181	P2P BitTorrent 傳輸

W8. LSAS 漏洞(LSAS Exposures)

W8.1 說明

Windows 2000、Server 2003 與 Server 2003 64 位元版、XP 及 XP 64 位元版上的 Windows 本地安全授權子系統服務(Local Security Authority Subsystem Service)有幾個嚴重的緩衝區溢位問題，如果被入侵成功，則系統會被完全控制。這個溢位問題被記載在微軟安全公告 MS04-011。攻擊者可由遠端匿名經由 RPC 對未修補的 Windows 2000 與 XP 系統發起攻擊，但仍需取得管理者權限才可成功。

Windows Server 2003 與 Windows XP 64 位元版本也具有此弱點，但所附的/GS 溢位保護功能即可防止 Sasser 網蟲造成**重大傷害**或完全佔領系統。

本地安全授權子系統服務(LSASS) 在身驗證與 Active Directory 的功能上扮演重要角色。當對 Active Directory 溝通介面送出異常的長字串時，LSASRV.dll 中的登入函式就會產生溢位。這個潛在問題會導致系統完全被佔領。

近期以 LSASS 為目標撰寫的 Sasser(又被稱為 W32.Sasser，請參閱 <http://www.cert.org/current/archive/2004/07/12/archive.html#sasser>、<http://www.microsoft.com/security/incident/sasser.mspx>)與 Korgo 網蟲(又被稱為 W32.Korgo，請參閱 <http://www.cert.org/current/archive/2004/07/12/archive.html#korgo>)帶給我們一個沉痛的事實，這個弱點可輕易由遠端侵入。許多近期的惡意自動網蟲利用這個弱點進行感染，它們對安全發展而言日益重要，但卻時常被人忽略。

這個弱點已被提報為 CVE 編號 CAN-2003-0533 項目。我們強烈建議網管人員不只要修補相關弱點，還要在網路節點上落實存取控制，以防 Windows RPC 的惡用行為進入脆弱的內部環境。

W8.2 受影響的作業系統：

Windows 2000, Windows XP and Professional, Windows XP 64 位元版本, Windows 2003

W8.3 CVE/CAN 項目

[CVE-1999-0227](#)

CAN-2003-0507, CAN-2003-0533, CAN-2003-0663, CAN-2003-0818

W8.4 如何得知你是否具有弱點:

這個弱點可由網路端或本機端發起檢查。由網路端發起可以方便安全與網路管理員對整個網段或 IP 範圍進行檢測，由本機端發起則是讓終端使用者可以自行檢查是否具有弱點。

這裏列出了幾種可由網路端進行檢查的免費工具：

1. Nessus 是一個網路型弱點評估軟體，具有一個 smb_kb835732.nasl 插件 (id 12209) 可以檢查是否更新了 KB835732。請由此網址查閱詳細說明並下載：
<http://cgi.nessus.org/plugins/dump.php3?id=12209>
2. FoundStone 釋出的 DSScan 可以掃描整個網段，並針對具有弱點的系統送出警告。請由此網址查閱詳細說明並下載：<http://www.foundstone.com/resources/proddesc/dsscan.htm>
3. eEye 出的 Sasser 網蟲掃描軟體可以找出目標系統是否會被 LSASS 攻擊或被 Sasser 網蟲病毒侵入。請由此網址查閱詳細說明並下載：
<http://www.eeye.com/html/resources/downloads/audits/index.html>

4. Microsoft Baseline Security Analyzer (MBSA) 可讓你知道主機是否具有此弱點。請由此網址查閱詳細說明並下載：<http://www.microsoft.com/technet/security/tools/mbsahome.mspix>

加強本機安全的推薦首選就是自動更新功能，以及下列微軟工具：

1. Microsoft Baseline Security Analyzer (MBSA)
<http://www.microsoft.com/technet/security/tools/mbsahome.mspix>
2. Windows 更新網站可以掃描你的電腦，並且告訴你還有哪些修補程式需要安裝。如果其中列出了 MS04-011 (KB835732)，則你的主機是具有此弱點的。詳細操作步驟請參閱：
<http://windowsupdate.microsoft.com>

W8.5 如何針對弱點進行防護

總論：

1. 由防火牆阻擋所有相關連接埠。
2. 套用微軟的最新修補程式。
3. 啟用系統上的進階 TCP/IP 篩選功能。

說明：

1. 由防火牆阻擋所有相關連接埠。

如果你有防火牆，請阻擋下列埠號以保護內部網路與系統不受外來攻擊影響：

- UDP/135, UDP/137, UDP/138, UDP/445
- TCP/135, TCP/139, TCP/445, TCP/593

管理 RPC 安全的最大障礙就是要管理 RPC 自身的訊息。RPC 服務通常使用暫用埠號，使得網路過濾器無法只憑特殊埠號找出 RPC 網路活動。一種可能作法是解析每個封包，看看它是否含有可辨識的 RPC 結構，但這會對過濾器造成沉重的負擔，相對地就不大實用。另一個可能作法是看看每個封包使用到的相關埠號是否落於常用 RPC 埠號範圍間，也就是 32,000 - 33,000。然而這可能會遺漏掉那些綁用在不同埠號的 RPC 封包。

建議可以使用個人防火牆，並阻擋所有主動內送的封包。如果你使用 Windows XP 或 Windows Server 2003 中的 Internet Connection Firewall (ICF)功能來協助保護網際網路連線，它預設就已阻擋了所有主動內送的封包。請依下列步驟使用網路安裝精靈來啟用 Internet Connection Firewall 功能：

- a. 點擊「開始」，再點選「控制台」。
- b. 在預設的類別目錄檢視中，點選「網路與網際網路連線」，點選「設定或變更你的家用網路或小型辦公室網路」。在使用網路安裝精靈設定好選項後，就代表了你的系統直接與網際網路連線，Internet Connection Firewall 功能會被自動啟用。

要手動為特定連線設定 Internet Connection Firewall 或 Windows 防火牆 (XP SP2)，請依下列步驟：

- a. 點擊「開始」，再點選「控制台」。
- b. 預設的類別目錄檢視中，點選「網路與網際網路連線」，點選「網路連線」。
- c. 在要啟用 Internet Connection Firewall 的連線上按右鍵，點選「內容」。

- d. 點選「進階」頁籤。
- e. 點選「以限制或防止來自網際網路對這台電腦的存取來保護我的電腦」，再點選「確認」。

注意：如果你想要讓某些程式或服務通過防火牆，請在「進階」頁籤中點擊「設定值」，接著選擇所需的程式、協定或服務。

2. 依 Windows 作業平台更新 LSASS 的修補程式。強烈建議使用 [自動更新](#) 功能。

LSASS 弱點修補程式可由微軟網站下載：

<http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx>

3. 啟用進階 TCP/IP 篩選器來阻擋所有對內封包。要設定 TCP/IP 篩選器，請依此步驟：
 - A. 點擊「開始」，點選「控制台」，在「網路連線」上按右鍵選擇「開啓」。
 - B. 在要設定內送存取控制的連線上按右鍵，點選「內容」。
 - C. 在「一般」頁籤「這個連線使用下列項目」下點選「Internet Protocol (TCP/IP)」，再點擊「內容」。
 - D. 在「Internet Protocol (TCP/IP) 內容」對話方塊中點擊「進階」。
 - E. 點擊「選項」頁籤。
 - F. 點選「TCP/IP 篩選」，點擊「內容」。
 - G. 勾選「啓用 TCP/IP 篩選(所有的介面卡)」。
 - H. 在「TCP/IP 篩選」對話方塊中有三個欄位，分別標示了：
 - TCP 連接埠
 - UDP 連接埠
 - IP 通訊協定

對每個欄位，你必須由下擇一：

- A. 全部允許。允許所有 TCP、UDP 或 IP 流量。
- B. 只允許。只允許指定的 TCP、UDP 或 IP 流量。點擊「新增」，在「新增篩選器」對話方塊中鍵入所需的通訊協定或埠號。若在「IP 通訊協定」中選取只允許 IP 通訊協定 6 和 17，就不能阻擋 UDP 或 TCP 流量。

注意：當設定 TCP/IP 篩選器時，請記得你需要阻擋哪些連接埠。LSASS 需要阻擋的是 TCP/445 連接埠。

[回首頁 ^](#)

W9. 收信軟體 (Mail Client)

W9.1 說明

微軟 Outlook 是微軟 Windows 負責管理個人訊息與收取電子郵件的客戶端程式。它主要負責管理信件，但也提供日曆、行事曆與通訊錄管理。當配合微軟 Exchange Server 時，微軟 Outlook 還可以提供額外的群組軟體功能，像是支援多使用者、幫助協調會議時間以及共享日曆與收件匣。

Outlook Express (OE) 是一個陽春的郵件與內容管理用戶端程式，從早期就隨附於 Internet Explorer - 從 Windows 95 開始，它就一直是所有微軟 Windows 系統的內部元件之一。最新版為 Outlook Express 6.0 SP1，可由 [微軟網站](#) 免費下載。微軟將 Internet Explorer 與 Outlook Express 整合到其他產品線時（包含 Office、BackOffice 與微軟的作業系統），就允許跨平台使用常用技術與程式碼。不幸的是，這種作法也造成了單一錯誤點問題，擴大了單一安全弱點能夠造成的影響。

微軟的目標是要發展出一套直觀可用的郵件與訊息管理解決方案。很不幸的，內建安全控制機制與

所嵌入的自動化功能格格不入，所以常被終端使用者忽略。這讓電子郵件病毒、網蟲、惡意程式有機會可以入侵本機系統或進行其他各式攻擊。

電子郵件用戶端軟體的潛在安全威脅包括：

- 感染電腦病毒或網蟲 – 惡意程式藉著附件與信件本文中內嵌的腳本程式碼進行散布。
- 垃圾郵件 Spam – 不請自來的電子廣告信件。
- 網頁信標 – 當收件者開啓信件時，其電子郵件位址就被確認為有效。

Outlook 與 Outlook Express 的最新版本可保護使用者免受上述威脅，前提是要設定正確。

W9.2 受影響的作業系統：所有版本的微軟 Windows 系統都含有 Internet Explorer 併 Outlook Express，因此都有潛在弱點。

想知道現在所使用的 OE 版本，請啓動 Internet Explorer，點選「說明」選單下的「關於 Internet Explorer」。版本小於 6 的話，應立即進行版本更新，並安裝所有安全修補程式。

Outlook 為使用者需要自行安裝的軟體，它可獨立安裝，也可與 Microsoft Office 套裝軟體一起安裝。微軟 Windows 下的 Outlook 版本有：

- Outlook 95
- Outlook 97
- Outlook 98
- Outlook 2000，又被稱為 Outlook 9
- Outlook XP，又被稱為 Outlook 10 或 Outlook 2002
- Outlook 2003，又被稱為 Outlook 11

微軟公司不再支援 Outlook 2000 之前版本，因此我們強烈建議儘快更新到最新的保固版本 (Outlook 2003, 2002 或 2000)。

所有版本的 Outlook 都應套用最新的產品服務套件。

Outlook 目前的服務套件版本為：

- Outlook 2000 - [Service Pack 3](#)
- Outlook XP (Outlook 2002) - [Service Pack 3](#)
- Outlook 2003 [Service Pack 1](#).

要知道現在所使用的 Outlook 版本，啓動程式並點選「說明」選單下的「關於 Outlook」。

參考資料：

Outlook Express <http://www.microsoft.com/windows/oe/>

Outlook <http://www.microsoft.com/office/outlook/>

產品生命週期 [http://support.microsoft.com/default.aspx?id=fh;\[ln\];lifeprodo](http://support.microsoft.com/default.aspx?id=fh;[ln];lifeprodo)

Microsoft Office 下載區 <http://office.microsoft.com/OfficeUpdate>

[CVE-2001-1088](#), [CVE-2002-0152](#) (僅針對 Macintosh), [CVE-2002-0685](#), [CVE-2002-1056](#)

[CVE-2003-0007](#), [CAN-2003-0301](#), [CVE-2004-0121](#), [CAN-2004-0215](#), [CAN-2004-0284](#), [CAN-2004-0380](#), [CAN-2004-0501](#), [CAN-2004-0502](#), [CAN-2004-0503](#), [CAN-2004-0526](#)

W9.3 如何得知你是否具有弱點

有安裝 Internet Explorer 的電腦就有安裝 Outlook Express。若曾手動安裝微軟 Office 套裝軟體，就可能在安裝常用套件 Word、Excel、PowerPoint 和 Access 時同時安裝 Outlook。

若具有下列情形，則系統就可能含有弱點：

- a. 未完全更新至最新版本，你可由 [Windows 更新網站](#) 測試
- b. 未適當設定安全選項

W9.4 如何針對弱點進行防護

你可以進行一些設定來降低 Outlook 與 Outlook Express 的安全風險。

保護 Outlook / Outlook Express 安全

Outlook 和 Outlook Express 每次發布新版本都增加了新控制項以有效保護使用者系統與隱私，因此確保用戶端程式與軟體的更新是很重要的。相關的更新可由下列方式取得：

1. 定期造訪微軟更新網站 <http://windowsupdate.microsoft.com>，套用所有重大修補程式。
2. 啟用 [自動更新](#) 以維護系統穩定性、完整性與 安全性。
3. 停用郵件預覽窗格，請打開「檢視--> 版面配置」選單，反勾選「顯示預覽窗格」。
4. 為內送郵件嚴格設定安全性區域。打開「工具--> 選項」選單，點擊「安全性」頁籤，點選「受限制的網站區域（較安全）」，並手動將相關設定調至高度安全性。點擊「套用」與「確定」。

預防可能藏有惡意程式的附件

Outlook 2000 (SP3)、Outlook 2002 (SP1 之後) 及 Outlook 2003 (所有版本) 都增加了對附件的防護，以防內含惡意程式碼。所有帶有 .exe、.com、.vbs 等副檔名的附件預設都會被阻擋。如果有需要傳送執行檔，請使用檔案壓縮軟體（如 WinZip）或其他的檔案傳輸方式 (FTP、SCP)。

Outlook 預設阻擋的副檔名清單可參考這份文件：

<http://www.microsoft.com/office/ork/2003/three/ch12/OutG07.htm>

如需增加阻擋的檔案型態清單，可依下列步驟所述修改登錄值：

1. 點擊「開始」、點擊「執行」、鍵入「regedit」，點擊「確認」。
2. 在登錄值中瀏覽下列機碼

Outlook 2003:

HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security

Outlook XP/2002:

HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Security

Outlook 2000:

HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Security

3. 開啓「編輯」選單，點擊「新增」，點選「字串值」。
4. 鍵入「Level1Add」，按下 ENTER 鍵。
5. 開啓「編輯」選單，點擊「修改」。

6. 鍵入所要設定的副檔名，點擊「確定」。

注意：: file_name_extensions 是附件副檔名清單。每個附件副檔名由半形分號區隔，例如要同時阻擋電子郵件中含有.zip 或.gif 檔案的附件，請鍵入「.zip;.gif」。

微軟 Technet 文章 KB837388〈如何設定 Outlook 封鎖其他的附件副檔名〉中記載了詳細的作法：

<http://support.microsoft.com/kb/837388/>

預防垃圾郵件(不請自來的電子廣告信件)

Outlook 2003 含有對垃圾郵件的有效防護。要設定這項功能，請啟動 Outlook，點選「執行 - 垃圾郵件 - 垃圾電子郵件選項」。

對話方塊中的「選項」頁籤有四個勾選項，這就是反垃圾郵件引擎的控制與門檻設定：

- 不自動篩選 - 不會篩選垃圾郵件。
- 低 (預設) - 頗有效的選項，可將最明顯的垃圾郵件移至垃圾郵件收件夾，誤判率非常低。
- 高 - 激進的篩選方式，會抓到絕大多數的垃圾郵件並送入垃圾郵件收件夾，但是也可能會抓到一些一般郵件。如果選定此選項，建議定期檢查垃圾郵件收件夾，看看有沒有被誤認為垃圾郵件的一般郵件。
- 僅安全的清單 - 只有「安全的寄件者清單」或「安全的收件者清單」上的人員或網域所寄出的郵件可以傳送至你的收件匣。這是最能預防垃圾郵件的選項，但需要耗費時間與心力去找出可能與使用者溝通的電子郵件位址，以建立「安全的寄件者清單」與「安全的收件者清單」。

Outlook Express 及舊版 Outlook 都沒有能有效防止垃圾郵件的功能，但可自訂「封鎖的寄件者清單」。要在 Outlook Express 設定這項功能，請打開「工具 --> 郵件規則」選單，並點選「封鎖的寄件者清單」。

預防電子郵件本文中內嵌的惡意程式碼

純文字信件中無法插入程式，但使用豐富文本(rich-text)格式(HTML、RTF)的電子郵件中，就有可能被內嵌惡意的程式碼。要預防這種程式碼，最簡單有效的方式就是以純文字格式閱讀信件。在 Outlook 2003 中請打開「工具 --> 選項」選單，點擊「偏好」頁籤，點擊「電子郵件選項」，點選「以純文字讀取所有標準郵件」和「以純文字讀取所有數位簽章的郵件」，點擊兩次「確認」。

預防網頁信標

網頁信標所用的手法就是在 HTML 格式信件中夾帶小圖檔 (通常為 1x1 圖點大小)，這是一種用以確認郵件信箱是否有效的機制。郵件一旦被開啓，就代表了可對收件者繼續寄送垃圾郵件。除了用以確認使用者開啓電子郵件外，網頁信標還可以獲得一些與使用者系統或自身相關的資訊(IP 位址、語系、瀏覽器版本)等。要在 Outlook 2003 上預防網頁信標，請啟動 Outlook，打開「工具-->選項」選單，點擊「安全性」頁籤，點擊「變更自動下載設定」勾選「不要自動下載 HTML 電子郵件中的圖片或其他內容」以及「在編輯、轉寄或回覆電子郵件時，在下載內容前先警告我」，點擊「確認」兩次。注意 Outlook 2002 已預設勾選這些選項，以協助保護使用者的安全與隱私。

使用者習慣

人的因素總是資安流程中最脆弱的一環，在處理電子郵件時遵循最佳指導原則是很重要的。

當收到附件時，即使是來自可信的來源，仍應依照下面「防毒」一節中的方法來檢查是否夾帶病毒或惡意程式。

在收到附件後，不要儲存到「我的文件」中，因為許多病毒是以這裏作為起始點。另存至其他資料夾，甚至另一個磁碟分割以隔離附件與其他檔案。

不要開啓未知的附件，即使是朋友寄來的。連 DOC 與 XLS 檔案都可能會內嵌 VMA 巨集傷害你的系統。如果你必需使用其他微軟產品（例如 Word）開啓，請在「工具 --> 選項 --> 安全性 --> 巨集安全性」中點選「高 - 未經簽章的巨集都會被自動停用」。在預設設定中，未經簽章的巨集不允許在系統上執行。

一定要檢查執行檔所附的電子簽章，以確保檔案完整性，並確認它的確是由可信來源所發出的。

防毒

防毒軟體可協助電腦預防大多數的病毒、網蟲、木馬及其他惡意程式。防毒軟體的病毒碼一週最少要更新一次，最好是天天自動更新，才能預防新種威脅。當今多數的防毒方案都會自動進行更新。更小心的作法是確保每個檔案都會被嚴密掃描，無論檔案類別或來源。

現在的防毒方案都有能力檢查進出的電子郵件，以阻擋惡意的檔案類別與腳本程式以免它們危害主機。

建議於使用電子郵件及網路服務前，先行安裝防毒工具並更新。因為許多病毒是以附件和惡意腳本程式碼的形式，透過電子郵件用戶端在使用者開啓或瀏覽信件時散布。

參考資料：

微軟防毒軟體參考資料 <http://www.microsoft.com/security/protect/antivirus.asp>

更新 Outlook 與 Outlook Express

Outlook Express 近年來被更新過數次，提供了更為強大的內建功能、穩定度與安全性。最新版可由微軟網站免費下載：<http://www.microsoft.com/Windows/oe/>，並附加於 XP Service Pack 2。

要維持 Outlook 及其他 Office 軟體的更新狀態，請造訪 [Office 產品更新網頁](#)。這個網站可自動檢查需要安裝的重大更新程式。

要瞭解 Office 2003 其他的安全功能與設定，請詳閱 [Office 2003 安全白皮書](#)。

注意：在對所轄電腦進行任何變更前，應通知系統管理者。管理者可在 [Office 資源工具包](#) 中找到與 Outlook 電子郵件安全更新相關的技術細節。

反安裝 Outlook

如果使用者有使用獨立電子郵件或訊息管理用戶端程式，則可將 Outlook 移除。

適用於所有 Windows 版本上的 Outlook

要移除 Outlook，請點擊「開始 --> 設定 --> 控制台」並雙擊「新增或移除程式」圖示。當跳出「新增或移除程式」對話方塊後，點選「Outlook」進行移除。

適用於 Windows 98/ME 的 Outlook Express

要移除 Outlook Express，請點擊「開始 --> 設定 --> 控制台」並雙擊「新增或移除程式」圖示。當跳出「新增或移除程式」對話方塊後，點擊「Windows 設定」頁籤，點選「Microsoft Outlook Express」進行移除。點擊「套用」與「確定」後，Windows 就會移除 Outlook Express。

適用於 Windows 2000/XP 上、或隨 Internet Explorer 更新後的 Outlook Express

使用者若想要移除 Windows 2000/XP，或隨瀏覽器更新到新版的 Outlook Express，步驟十分複雜。細節請參考下列的微軟文件：

使用微軟 Outlook Express 5.x/6.0 版的 Windows 2000 使用者
<http://support.microsoft.com/kb/263837>

使用微軟 Outlook Express 5.x/6.0 版的 Windows 98/Me 使用者
<http://support.microsoft.com/kb/256219>

注意：Outlook Express 可能在安裝服務套件、程式包或更新作業系統的同時被自動重新安裝。

[回頁首 ^](#)

W10. 即時通訊(Instant Messaging)

W10.1 說明

即時通訊技術這幾年來已日趨成熟，早期它只是一種讓使用者與親友能快速保持聯繫的神奇附加程式，今日它已成爲 Windows 作業系統核心功能之一，廣泛用於商業通訊、合作及輔助營運。當第三方即時通訊程式仍佔有大部分市場時，將即時通訊功能整合到作業系統中的趨勢也慢慢成形，同時也爲那些使用安全政策或安全作業架構來限制這項技術的公司直接帶來潛在安全危險。這些程式的弱點更是大大地威脅到那些缺乏反制技術、安全人員及相應設備的組織，讓他們疲於應付日益增加的內在威脅。

到目前爲止，Windows 系統上最主要的 IM 程式爲 Yahoo! Messenger (YM)、AOL Instant Messenger (AIM)、MSN Messenger (MSN) 與 Windows Messenger (WM)，後者已經完全整合在 Windows XP Professional 與 Home 版本中。這些桌上型程式爲使用者帶來了各式各樣的功能，像是遠端檢查網頁郵件、語音交談、視訊通訊、傳送分享檔案及純文字交談。另外還有一種「混用式網路」通訊程式，讓使用不同訊息網路或協定的使用者可透過中央介面彼此交談，相關例子有 Trillian、以及最近的 AOL、Yahoo!、MSN 聊天聯盟，可讓三種 IM 軟體的用戶端在同一個工作場所內無障礙地進行交談。

這些程式及相關功能具有可被遠端入侵的弱點，逐漸威脅到網路安全及完整性，尤其是它們持續整合並布署在 Windows 系統中的比例越來越重。對即時通訊弱點進行攻擊的案例隨處可見，包括了遠端執行緩衝區溢位(以 RPC 爲主的異常封包)、URI/惡意連結攻擊、檔案傳輸弱點及 Active X 攻擊程式。

這些程式的弱點通常分爲幾個大類：

- 舊版的 ActiveX 控制項 – 例如 MSN Messenger "ResDLL" 緩衝區溢位([CAN-2002-0155](#))、Yahoo! Voice Chat ActiveX 控制項緩衝區溢位弱點(<http://www.securityfocus.com/bid/7561>)、Yahoo! Webcam ActiveX 控制項緩衝區溢位弱點(<http://www.securityfocus.com/bid/8634>)。
- URI 實作問題 – 例如 Yahoo! Messenger 執行惡意腳本程式碼([CAN-2002-0032](#))、Yahoo! Messenger URI 處理器緩衝區溢位([CAN-2002-0031](#))。
- 各種緩衝區溢位，像是因爲檔案傳輸所造成的問題 – 例如 MSN Messenger 檔案確認失敗([CAN-2004-0122](#))、Yahoo! Messenger 「Imvironment」與「message」欄位分別具有緩衝區溢位([CAN-2002-0320](#) 與 [CAN-2002-0320](#))、AOL Instant Messenger TLV 0x2711 套件解析緩衝區溢位([CAN-2002-0005](#)、[VU#912659](#))、Yahoo! Messenger YAuto.DLL Open 緩衝區溢位

弱點 (<http://www.securityfocus.com/bid/9145>)、AOL Instant Messenger Getfile Screenname 緩衝區溢位弱點 (<http://www.securityfocus.com/bid/8825>)。

這些程式不只具有網路與系統上的弱點，同時也有洩露智慧財產、機密資訊，或降低員工產能的風險。清除程式弱點固然重要，訂立可用的網路安全政策來限制內外流量也是刻不容緩的，如此才能防止即時通訊曝露在網際網路上的問題。

W10.2 受影響的作業系統：

Windows 98、Windows ME、Windows 2000 Professional, Windows XP 與 Windows 2003 都可執行微軟 Instant Messenger。微軟 Windows XP 所有作業系統版本都附加了 Instant Messenger。

W10.3 CVE/CAN 項目：

[CVE-2002-0005](#), [CVE-2002-0032](#), [CVE-2002-0155](#), [CVE-2002-0785](#), [CAN-2004-0636](#)

[CAN-2002-0031](#), [CAN-2002-0228](#), [CAN-2002-0320](#), [CVE-2002-0362](#), [CAN-2003-0717](#), [CAN-2004-0043](#), [CAN-2002-1486](#)

W10.4 如何得知你是否具有弱點：

要知道目前所安裝的微軟 Instant Messenger 版本，啟動程式後開啓「說明」選單，點選「關於 Instant Messenger」。小於 6.2 版的使用者應立即進行昇級並安裝最新修補程式。

W10.5 如何針對弱點進行防護：

- a. 確認所安裝的所有即時通訊軟體，像是 Yahoo、MSN、AOL、Trillian 等都已依廠商指示套用最新修補程式。
- b. 設定入侵防禦/偵測系統，在發現使用即時通訊軟體傳送檔案時發出警訊。
- c. 如果安全政策允許，請由防火牆阻擋下列連接埠。注意這不是完整的安全措施，因為某些程式仍能避過防火牆。
 - o 1863/tcp：微軟.NET Messenger、MSN Messenger
 - o 5050/tcp：Yahoo Messenger
 - o 6891/tcp：MSN Messenger 檔案傳送
 - o 5190-5193/tcp：AOL Instant Messenger
- d. 阻止對網址列中含有「aim:」或「ymsgr:」的網頁進行存取，這可以防止對 URI 處理器弱點的利用。另一個方式是小心移除「HKEY_CLASSES_ROOT」機碼內的對應登錄值。
- e. 阻擋任何會觸發與即時通訊軟體相關 Active X 控制項的網頁存取活動。這可以防止對相關 Active X 控制項弱點的利用。

[回頁首 ^](#)

Top Vulnerabilities to UNIX Systems (U)

U1. BIND 域名系統(BIND Domain Name System)

U1.1 說明

柏克萊大學網際網路名稱網域(BIND)程式套件已經成為世界上域名系統(DNS)最廣為採用的軟體。DNS 是協助將主機名稱(例如 www.sans.org)轉換成所對應註冊網路位址(IP)的重要系統。

許多 DNS 伺服器都與網際網路界接，因此也成為攻擊者最愛的目標。即使這些伺服器對企業來說十分重要，但有研究指出現今仍在提供服務的主機中，絕大部分都版本過舊、設定錯誤或具有弱點 [1]。因此，許多伺服器都可被過去幾年所發布過的攻擊手法侵入，包含了阻絕服務(亦即使用特製的 DNS 要求或回應封包癱瘓名稱服務程式)、緩衝區溢位攻擊與快取汙染，雖然 BIND 發展小組對

於相關問題及弱點修復的回應一直都非常迅速。

U1.2 受影響的作業系統：

每種 UNIX 與 Linux 系統散布時都包含了某個版本的 BIND，Windows 平台上也有。

U1.3 CVE/CAN 項目

[CVE-1999-0009](#), [CVE-1999-0024](#), [CVE-1999-0184](#), [CVE-1999-0833](#), [CVE-1999-0837](#), [CVE-1999-0835](#), [CVE-1999-0848](#), [CVE-1999-0849](#), [CVE-1999-0851](#), [CVE-2000-0887](#), [CVE-2000-0888](#), [CVE-2001-0010](#), [CVE-2001-0011](#), [CVE-2001-0012](#), [CVE-2001-0013](#), [CAN-2002-0029](#), [CAN-2002-0400](#), [CAN-2002-0651](#), [CAN-2002-0684](#), [CAN-2002-1219](#), [CAN-2002-1220](#), [CAN-2002-1221](#), [CAN-2003-0914](#)

U1.4 如何得知你是否具有弱點

任何使用作業系統內附 BIND 版本的 DNS 伺服器都應檢查相關廠商提供的最新修補程式。如果安裝的是由 [Internet Software Consortium \(ISC\)](#) 原始碼編譯而的 BIND，則應確認是否安裝最新版。版本過舊或未修補的 BIND 版本通常都有弱點。

在多數的系統實作下，「named -v」指令可以顯示所安裝的 BIND 版本，格式為 X.Y.Z，X 是主版本、Y 是子版本、Z 則是更新等級。目前主要的三個 BIND 版本為 4、8 和 9。如果所執行的 BIND 伺服器是由原始碼所建成，則應避免使用第 4 版，而最好採用第 9 版。你可以由 [ISC](#) 下載最新的 9.3.0 版。

保護 BIND 安全的其中一種預防方式就是訂閱相關公告或弱點報告，像 [SANS](#)、[Secunia](#) 都會持續在 [OSVDB](#) 上發表通報。除了安全預警外，更新後的弱點掃描軟體也可有效診斷出 DNS 系統上的潛在弱點。

U1.5 如何針對弱點進行防護

- 一般針對 BIND 弱點的防護方式：
 1. 套用所有廠商更新程式，或更新 DNS 伺服器的版本。想要進一步知道有關強化 BIND 安裝的細節，請參閱下列連結中有關保護名稱服務安全的參考資料：[CERT 的 UNIX 安全檢查表](#)。
 2. 為任何位於內網，不需讓網際網路存取的 DNS 伺服器設定相應的防火牆規則。
 3. 利用加密管道來保護主伺服器與次伺服器間的區域傳送(zone transfer)活動，設定伺服器使用 DNS 交易簽章 (TSIG)。BIND 8.2 之後才提供 TSIG 選項。
 4. 禁錮(Jail)：要避免 BIND 服務被入侵後影響到整個系統，可將 BIND 限制使用無權限使用者執行，並禁錮在 chroot()後的目錄中。BIND 9 的作法可參考 <http://www.losurs.org/docs/howto/Chroot-BIND.html>。
 5. 停用遞歸查詢(recursion)於順手擷取(glue fetching)功能，以防止 DNS 快取汙染。
- 針對近年來被發現的 BIND 弱點進行防護：
 1. 透過負向回應快取汙染：<http://www.kb.cert.org/vuls/id/734644>
 2. 針對 ISC BIND 9 的阻絕服務弱點：<http://www.cert.org/advisories/CA-2002-15.html>
 3. 針對 ISC BIND 8 的阻絕服務弱點：<http://www.isc.org/products/BIND/bind-security.html>

今日已經有許多關於強化 BIND 的優良手冊，其中一份手冊談及了如何強化 Solaris 系統上的 BIND，與其他可進一步參考的 BIND 連結都可在 [〈安心使用 BIND9 DNS 伺服器〉](#) 上瀏覽。BIND 安全文件被儲存於 [AFENTIS](#)。你也可以在下列網址中瀏覽有關 BIND 通用安全的實務，其中也包含了 TSIG：

http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf.

參考資料：

[1] DNS 伺服器研究

<http://mydns.bboy.net/survey/>

[回頁首 ^](#)

U2. 網頁伺服器 (Web Server)

U2.1 說明

HTTP 是公眾網路上最常使用的網路活動，Unix 網頁伺服器是此服務的主要提供者，像是 Apache 與 Sun Java System Web Server (前身為 iPlanet)，因此在安全事務上也最需小心戒慎。相關的問題包含了伺服器本身與增益模組的弱點、預設/範例/測試用的 cgi 腳本程式、PHP 程式問題及各式各樣的攻擊手法。

在這麼多種 Unix 網頁伺服器威脅中，最常被利用、也是發生最多次的成因就是安裝時的錯誤設定及缺乏定期維護。疏忽結果可能導致任何問題，從阻絕服務、網頁被置換、到攻擊者取得伺服器上的 root 權限，以及任何其他可能的威脅。

各大廠商與開放原始碼計畫都為自家產品提供了最佳實務設定方式並持續進行安全更新，對網站管理員而言，掌握最新相關資訊是十分重要的。要知道，大部分出事的網頁伺服器，都是被公開的攻擊程式利用廠商發布已久的弱點入侵。

U2.2 受影響的作業系統

所有 UNIX 系統都可執行 HTTP 伺服器。許多由 Linux 與 UNIX 繼承而來的系統都會預設安裝且啟用 Apache。除此之外，Apache 和 iPlanet/Java System 還可以在其他作業系統上執行，所以也會受到相同弱點影響。

U2.3 CVE/CAN 項目

注意：如前所述，Apache 與 iPlanet/Java System 都可以在多種作業系統上執行。這些伺服器上的使用者應仔細翻閱下方的「CVE/CAN 項目」，以及在 W1.3 小節中所述的 Windows 列表，以確保處理到每個弱點。

Apache

[CVE-1999-0021](#), [CVE-1999-0066](#), [CVE-1999-0067](#), [CVE-1999-0070](#), [CVE-1999-0146](#), [CVE-1999-0172](#), [CVE-1999-0174](#), [CVE-1999-0237](#), [CVE-1999-0260](#), [CVE-1999-0262](#), [CVE-1999-0264](#), [CVE-1999-0266](#), [CAN-1999-0509](#), [CVE-2000-0010](#), [CVE-2000-0208](#), [CVE-2000-0287](#), [CAN-2000-0832](#), [CVE-2000-0941](#), [CVE-2002-0061](#), [CVE-2002-0082](#), [CVE-2002-0392](#), [CAN-2002-0513](#), [CAN-2002-0655](#), [CAN-2002-0656](#), [CAN-2002-0657](#), [CAN-2002-0682](#), [CAN-2003-0132](#), [CAN-2003-0189](#), [CAN-2003-0192](#), [CAN-2003-0254](#), [CAN-2004-0488](#), [CAN-2004-0492](#)

iPlanet/Sun Java System Web Server

[CVE-2000-1077](#), [CAN-2001-0419](#), [CAN-2001-0746](#), [CAN-2001-0747](#), [CAN-2002-0686](#), [CVE-2002-0845](#), [CAN-2002-1315](#), [CAN-2002-1316](#)

OpenSSL

[CAN-2003-0543](#), [CAN-2003-0544](#), [CAN-2003-0545](#)

PHP

[CVE-2002-0081](#), [CAN-2003-0097](#), [CAN-2004-0594](#)

其他

[CAN-2004-0529](#), [CAN-2004-0734](#)

U2.4 如何得知你是否具有弱點

任何使用預設安裝，或未進行修補的網頁伺服器都應視為具有弱點。持續追蹤最新安全問題的最佳方式就是查閱廠商的安全資訊網頁，以下是一些範例：

- Apache HTTP 伺服器 [首頁](#)與 [安全報告](#) (包含了通往 [ApacheWeek](#) 的連結)。
- [Sun 網頁、入口與目錄伺服器下載中心](#) 與 [BigAdmin 入口網頁](#)。
- [PHP 首頁](#)與 [下載區](#)。
- [OpenSSL](#)

以下列出的弱點都應立即進行處置。從弱點公布到攻擊程式公開、再到攻擊程式被改寫成爲網蟲，其間的時間是越來越短。你可藉由弱點掃描軟體來協助進行弱點評估，像是 [Nessus](#) 與 [SARA](#)（均爲開放原始碼軟體）或 [eYE](#) 所提供的[免費工具](#)及[商用掃描軟體](#)。管理者應由網路端進行掃描，以同時找出已知及未知伺服器所帶來的風險。

U2.5 如何針對弱點進行防護

1. 確保所有網頁伺服器都已具有最新修補等級，請參閱「如何得知你是否具有弱點」一節中相關廠商的網頁連結。
2. 停用伺服器上部分或所有不需使用的功能，尤其是 CGI 存取、php、mod_ssl 與 mod_proxy (針對 Apache)。請預設先停用它們，待服務需要時再行啓用。
 - 如果必需使用 PHP、CGI、SSI 或其他腳本程式語言，請考慮配置 suEXEC。suEXEC 可以讓腳本程式執行時的使用者有別與 Apache 使用者。
 - **警告：**使用 suEXEC 前一定要充份瞭解設定方式，配置不當會導致新的安全漏洞。
3. 使用 Apache 1.3.x 的話，請參閱 <http://httpd.apache.org/docs/suexec.html>
4. 使用 Apache 2.0.x 的話，請參閱 <http://httpd.apache.org/docs-2.0/suexec.html>
5. 保護 cgi-bin 與其他腳本程式目錄的安全。應移除所有範例及預設的腳本程式。
6. 保護 PHP 安全：

這個問題本身就是個大哉問。下面列出幾點 PHP 安全實作的初步守則：

 1. 停用 PHP 中會讓 HTTP 標頭洩露資訊的參數。
 2. 確保 PHP 以安全模式執行。

詳細說明可參閱：
<http://www.securityfocus.com/printable/infocus/1706>
7. 有些模組也可以幫助保護 Apache 安全。mod_security (www.modsecurity.org) 模組可以協助預防跨網站腳本程式碼攻擊 (XSS) 及 SQL 注入 (SQL injection)。詳細實作步驟請參閱他們的網站。
8. 對腳本程式稽核 XSS 與 SQL 注入弱點也很重要。有一些開放原始碼工具可以幫上忙。Nikto (可由 <http://www.cirt.net/code/nikto.shtml> 取得) 就是一個合用的 CGI 掃描工具。
9. 考慮在 chroot 環境中執行 HTTP 伺服器，被 chroot 後，HTTP 伺服器就不能存取作業系統上的其他目錄結構。這樣作可以限制攻擊程式的活動。舉例來說，攻擊程式可能會試圖開啓 shell，但因爲 /bin/sh 通常不存在於 (也不應該在) chroot 環境中，開啓動作就會失敗。**警告：**對需要存取網頁伺服器上其他函式庫或程式的 CGI、PHP、資料庫及其他模組或通訊連線的元件來說，使用 chroot 可能會造成負面影響。Choort 有許多作法，請先閱讀其軟體說明文件以協助進行。進一步資訊可查閱：
 - <http://www.w3.org/Security/Faq/wwwsf3.html#SVR-Q5>
 - <http://www.modsecurity.org/documentation/apache-internal-chroot.html>
 - http://www.sun.com/software/whitepapers/webserver/wp_ws_security.pdf
10. 不要使用 root 帳號或其他具有超級使用者權限的帳號來執行網頁伺服器。請開一個具有最小權限的獨立群組與帳號來執行網頁伺服器，這個群組與帳號不該執行其他程式 (例如執行 Apache 時，使用 apache 帳號來取代 nobody 帳號)。
11. 限制可能洩露的伺服器資訊。

這個建議會與風險管理的安全建議相衝突，資訊不足無助於降低安全風險，而許多公眾網路上的攻擊程式通常都採用盲目的無差別攻擊 (你可以在許多 Apache 記錄檔中找到 IIS 攻擊痕跡)。不過也有某些攻擊程式的確是以標頭資訊作爲觸發條件。

 - 修改預設的 Apache HTTP 回應表徵：

1. 使用 Apache 1.3.x 的話，請參閱
<http://httpd.apache.org/docs/mod/core.html#servertokens>
<http://httpd.apache.org/docs/mod/core.html#serversignature>.
 2. 使用 Apache 2.0.x 的話，請參閱
<http://httpd.apache.org/docs-2.0/en/mod/core.html#servertokens>.
- 確保網路網路無法存取到 `mod_info`。
 1. 關閉目錄瀏覽功能。
12. 在網頁伺服器上啟用有效並徹底的記錄機制，是對追蹤潛在問題與不明意圖的最佳方式。最好的作法是定期輪替記錄檔，並儲存舊的記錄，這可以讓記錄檔大小更容易管理和分析。
- 使用 Apache 1.3.x 的話，請參閱 <http://httpd.apache.org/docs/logs.html>
 - 使用 Apache 2.0.x 的話，請參閱 <http://httpd.apache.org/docs-2.0/logs.html>

在許多情形下這些記錄並不足夠，特別是使用 PHP、CGI 或其他腳本程式時，因此最好能夠記錄所有 GET 和 POST 活動。當發生入侵事件時，這就是最重要的資料與證據。你可以透過 `mod_security` (針對 Apache) 來記錄 GET 與 POST 活動。

- <http://www.modsecurity.org>
- <http://www.securityfocus.com/infocus/1706>

[回頁首 ^](#)

U3. 身分驗證(Authentication)

U3.1 說明

使用者與資訊系統間的每次交談幾乎都會用上密碼字串、密碼短語或安全驗證碼。多數的使用者認證形式、檔案及資料的保護機制都是依靠使用者密碼。驗證成功所進行的存取行為通常未加記錄，這樣的記錄也不容易讓人生疑，因此密碼洩露就成了一種難以被系統察覺的攻擊。攻擊者有權存取具有受害者權限的所有資源，甚至可以存取其他帳號、鄰近主機或管理者權限。儘管有這種安全威脅，使用脆弱密碼或空白密碼的例子仍然極為常見，有訂立密碼安全政策的組織更是少之又少。常見的密碼弱點有：

- a. 使用者使用脆弱密碼或無密碼。
- b. 使用廣為人知或自行公開的密碼
- c. 作業系統或第三方應用程式會新增具有脆弱密碼或無密碼的帳號。
- d. 多數商業或開放原始碼的應用程式都使用公開的雜湊演算法(hashing algorithm)，而密碼雜湊值(hash)儲存於一般使用者均可存取的地方。

預防密碼弱點的最佳方式是制定好的密碼政策，政策中應包括：教導使用者如何選用強韌密碼的詳細指示、要求使用者保管並定期更換密碼的明確規定、一套讓資訊人員可立即更換脆弱/不安全/預設及通用密碼，同時鎖定不使用/無活動等帳號的作業方式、還有一套預防流程可以定期檢查密碼強度與複雜度，移除不需要使用的預設使用者或管理者帳號，及定期檢視系統存取與認證記錄檔。請由此網址查閱 Unix 設定通用手冊：http://www.cert.org/tech_tips/unix_configuration_guidelines.html

U3.2 受影響的作業系統：

所有利用使用者 ID 與密碼進行驗證的作業系統與應用程式。

U3.3 CVE/CAN 項目

[CAN-1999-0501](#), [CVE-1999-0502](#), [CAN-1999-1029](#), [CVE-2001-0259](#), [CVE-2001-0553](#), [CVE-2001-0978](#), [CVE-2001-1017](#), [CVE-2001-1147](#), [CVE-2001-1175](#), [CAN-2004-0243](#), [CAN-2004-0653](#)

U3.4 如何得知你是否具有弱點

1. 檢查常用帳號：
 - 如果有多人共用或使用者暫用的帳號，且密碼是公布在筆記、桌上或螢幕上，則對任何可接觸到實體系統的人來說，這都是存取內網的一條大道。
2. 檢查是否使用脆弱密碼，或選取密碼的方式過於脆弱：
 - 如果為新增使用者帳號指定相同或易猜測的初始密碼，即使在首次登入後可更改密碼，都已給予攻擊者一個存取系統的良機。
 - 檢查密碼雜湊值儲存於本機的 `/etc/passwd` 還是 `/etc/shadow`。為了讓網路使用者進行驗證，所以 `/etc/passwd` 必需讓所有帳號都有權讀取。如果這個檔案中含有密碼雜湊值，則任何可存取系統檔案的使用者都可以讀取雜湊值，並使用密碼破解器來破解。`/etc/shadow` 被設計為只有 `root` 可以讀取，並只能用於儲存密碼雜湊值。如果本機帳號未被 `/etc/shadow` 保護，則它們的密碼就遭受極大風險。除非安裝者另有指定，否則新的作業系統大多數都預設採用 `/etc/shadow` 來儲存密碼雜湊值。你也可以使用 MD5 演算法來產生密碼雜湊值，會比舊有加密演算法來得安全。
3. NIS 環境：
 - 網路資訊服務(NIS)是一群以資料庫形式提供的服務程式，用以將位址資訊（稱為地圖）提供給其他網路服務，網路檔案系統(NFS)就是其中一種。在原本設計中，NIS 密碼雜湊值會寫入 NIS 設定檔裏並供所有使用者讀取，因而產生了密碼風險。某些以 LDAP 為實作方向的網路認證服務中也具有相同問題。除非安裝者另有指定，否則新的 NIS 作法（例如 NIS+或 LDAP）對密碼雜湊值的保護通常較為嚴謹。然而這些新作法的設定方式可能過於困難，讓使用者望之卻步。
4. 一般考量：
 - 即使密碼雜湊值受到 `/etc/shadow` 或其他實作方式保護，還是可以使用其他方法猜到密碼。密碼常見的弱點之一就是離職員工帳號。在沒有標準流程提醒管理者注意的情況下，一般公司通常會忽略要停用舊的使用者帳號。
 - 只要使用作業系統或網路程式的預設安裝方式（無論是廠商還是管理者所為），就有可能產生大量未使用，且未來也不需使用的服務帳號。因為對作業系統或是應用程式不夠瞭解，導致在多數情況下廠商或管理者會事先安裝所有軟體，以防未來有不時之需。這簡化了安裝流程，但也同時製造了許多使用預設/脆弱/已知密碼的未使用服務與帳號。
 - 若密碼以明文在網路上傳送，例如使用 telnet、FTP 或 HTTP，則會讓惡意使用者有機會進行竊聽。像是 OpenSSH 或 SSL 之類的加密連線方法可以隱藏密碼，防止有心者監看網路。

U3.5 如何針對弱點進行防護

預防密碼弱點的最佳方式是制定好的安全政策，教導使用者養成良好的密碼習慣，並在公司許可下，由系統管理員定期事先檢查密碼的完整性。這裏列出了良好密碼政策的指導方針：

1. 保護強韌密碼。

只要硬體夠好、時間足夠，任何密碼都可被暴力猜測破解。密碼破解器使用的一種方式稱作字典攻擊法(Dictionary attack)。因為密碼加密方式是公開的，破解工具只要將所獲得的加密值與字典單字(可由各種語言中選取)所產生的加密值相比對，即可猜出原始密碼。所比對的單字還可與名字組合，或重新排列以擴展選擇範圍。用已知單字而造出的密碼是很容易被猜解出來的。許多組織都規定使用者密碼除了純字母之外，還要混用特殊符號，因此許多使用者就將原來的單字密碼(password)用特殊符號取代部分字元(pas\$\$w0rd)。這種轉換並無法防止字典攻擊，pa\$\$w0rd 仍會被解為 password。

好的密碼來源不該包含單字或名字。強韌的密碼政策應該告訴使用者用更隨機的方式來選擇密碼素材，像是一句話、書名或歌名。使用者可藉著將句子連結成長字串(像是將每個單字的第一個字母連在一起、或取代單字中的某些字母、移除所有母音等)，而造出一個夠

長，且包含純字母與特殊字元的密碼，讓字典攻擊法難以破解。如果原本的句子很難忘記，則轉換出來的密碼也一樣刻骨銘心。

一旦制定了密碼產生規則，安全政策就要落實以確保使用者遵循這個流程。最好的方式就是在使用者變更密碼時就對密碼進行檢查。UNIX/LINUX 愛用者可以用 Npasswd 作為前端檢查器，檢查輸入的密碼是否符合安全政策。啓用 PAM 的系統也可擴增使用 cracklib（一群隨附於 Crack 的函式庫），在密碼生成時進行檢查。大部分使用 PAM 的系統上也可以設定拒絕接受不符合規定的密碼。

若無法使用 Npasswd，或在 PAM 函式庫輸入密碼時無法使用字典函式庫檢查，管理者的標準防範程序中就應該規劃在獨立模式下執行破解工具。攻擊者愛用的工具也是你的首選，這包含了 UNIX/LINUX 平台上的 Crack 與 John the Ripper。

請注意：若無長官允許，絕對不要使用任何密碼破解器，即使是針對你有 root 權限的系統。許多好心的管理者因為未經授權執行密碼破解器而被開除。許可權需以書面記載，密碼安全政策中需明列此格式，並允許定期進行密碼檢測。

一旦你獲得執行密碼破解器的許可，請定時在安全的獨立主機或受實機保護的主機上執行。主機上的破解工具應限制只有經過授權的系統管理者才可以使用，嚴禁公開讓所有使用者存取。秘密通知密碼被破解成功的使用者，同時告知選擇良好密碼的方式。系統管理員與公司管理者必需合作研擬相關流程，以便在使用者不肯合作時，請公司管理者出馬協助。

另外一些能夠防止未設密碼或脆弱密碼的方法就是(a)改用其他驗證方式，像是密碼生成憑證或生物辨識。若你有脆弱密碼的問題，給予使用者另一種辨識方式是十分有效的。要注意為密碼生成憑證制定處理流程，以確保憑證不會被未授權的使用者取得；若憑證被偷，則應立即拒絕進入。生物辨識則是仍在發展中的概念，依驗證方式各有不同（例如指紋或臉形），某些技術仍未成熟，且驗證時經常發生錯誤。(b) 有許多第三方的免費或商用軟體都可協助管理良好密碼政策。

2. 保護強韌密碼。

如果你將密碼雜湊值存在 /etc/passwd，請將系統升級使用 /etc/shadow。如果你的系統上有執行 NIS 或 LDAP，且無法保護密碼雜湊值，則任何人（包含未經身分驗證的使用者）都可以讀取密碼雜湊值並破解。你應該尋求替換方案以取代現用的 NIS 或 LDAP 版本。在這些不安全的程式被替換或強化前，應確實檢驗正確的權限設定，並定期針對這些程式進行預防性破解。請考慮使用 MD5 演算法來代替 crypt 進行密碼雜湊的計算。

即使密碼夠強韌，使用者若不好好保管密碼，帳號還是會被盜用。良好的安全政策應該告訴使用者千萬別隨便透露密碼、不要將密碼寫在別人看得到的地方、並保護好自動驗證時會儲存的密碼檔案(例如開啓自動登入功能，最好的保護方式就是避免這類設定，只有在需要時才鍵入密碼)、若密碼外洩或被其他人得知，應立即通知管理者。落實密碼有效期的政策，不要使用舊密碼，即使密碼外洩，也只有短期間能造成影響。在密碼到期前就該警告使用者，並請他們更改密碼，因為使用者在突然看到「你的密碼已到期，必須馬上進行更改。」訊息時，通常會傾向選擇簡單好記的密碼。

3. 嚴格控管帳號。

這裏列出一些可以保證帳號被嚴格控管的評斷方式：

- 任何未使用的服務程式帳號、管理帳號或程式預設帳號應被停用或移除。
- 任何使用中的服務程式帳號、管理帳號或程式預設帳號應在安裝或啓用時更新成強韌密碼。

- 為新增使用者設定隨機產生的初始密碼，並強迫使用者在第一次登入後變更。
- 定期稽核所有系統上的帳號，並列出一份所有帳號的管理清單，詳細記載服務程式所需帳號及其用途。
- 定期檢查帳號是否仍需使用。
- 訂立作業流程以將認可帳號加入清單、並移除不使用的帳號。
- 員工或合約人離職，且帳號不再需要時，一定要有相關流程以確實移除其帳號。
- 與人事部門保持連繫，注意離職動態。
- 定期檢查清單是否需加入新帳號或移除舊帳號。

除此之外，不要忘記檢查路由器、網路數位印表機、影印機和印表機連接器等系統上的帳號密碼。如果這些設備未落實密碼管理，且某些使用者慣於使用與 UNIX 系統相同的密碼，則就可能為惡意使用者大開方便之門。

你可以在這個網址找到各家廠商產品的預設密碼：<http://www.cirt.net/cgi-bin/passwd.pl>

4. 加密登入

如果密碼是以明文形式在網路上傳輸，則再強韌的密碼也無用武之地，因為密碼可以被網路上的任何人看到。使用明文來傳送密碼的程式或協定包含了 telnet、FTP、HTTP 和柏克萊的 r 服務程式群。

要預防這個問題，就應該採用加密程式或協定，讓密碼不要以明文形式在網路上傳輸。這樣一來使用傳統的竊聽方式就難以擷取到密碼。

上述程式或協定的加密替代方案有許多種。OpenSSH 可以取代 telnet、FTP 與柏克萊 r 服務程式群，而 SSL 為 HTTP 協定提供了加密功能。

5. 超級使用者帳號

root 帳號是 Unix 系統上權限最高的帳號。它並沒有安全限制，意即你可以在系統上進行任何工作。這是惡意使用者最想要得到的帳號！

- 不要允許遠端登入 root。使用者應該用 su 指令來切換 root 權限。su 可以將帳號的有效 sid 變更為另一個，因此可用以切換成 root 帳號。
- 如果使用者只需使用部分特權指令，則可使用 sudo。sudo(superuser do)讓系統管理者可以開放某些指令給使用者，讓他們以 root 身分執行該指令，並記錄所下的指令與參數。使用者無需輸入 root 密碼。
- root 帳號只限用於安裝系統、設定應用程式、進行特殊設定或緊急用途。
- 限制 root 密碼的存取。密碼只能讓具有負責系統管理工作的人知道。

關於 sudo 的進一步資訊可參閱 <http://www.courtesan.com/sudo/>，關於 su 的資訊則請在命令列下鍵入 man su 觀看。

6. 通用帳號

通用帳號通常為程式開發時，讓應用程式得以跟其他應用程式或資料庫進行通訊所使用的帳號。通用帳號的另一個用途是提供廠商存取權限。這些帳號必需格外留意管理，記錄其所進行的任何活動。

一般處理方式

- 先停用，不得已時才啟用。如果使用者需要頻繁或長時間使用，應幫他指定專屬帳號。
- 如果必需使用通用帳號（像是廠商要求允許多個使用者能夠存取、或應用程式具有認證存取的功能），每次身分驗證完後都要完整記錄該帳號的活動。

應用程式帳號

- 不要將密碼寫入程式碼中。
- 對帳號密碼資訊進行充份保護（利用檔案加密、讀取權限等）。

廠商存取權限

- 需廠商同意帳號可被稽核，並簽署支援帳號同意書。
- 指名一位廠商密碼監管人，負責管理廠商密碼。
- 彌封支援帳號的密碼，廠商需來電詢問後才可取得。
- 儘可能使用雙重驗證方式。
- 當密碼使用後，儘可能要求廠商密碼監管人更換密碼。如果使用雙重驗證則不一定要進行此步驟。
- 確認彌封密碼未被變更。
- 定期稽核帳號活動。

稽核軌跡(Audit trail)

保留使用者活動的稽核軌跡對系統防護來說是很重要。無論身分驗證是否成功，完整的記錄有助於你找出系統哪裏還需要補強。記錄 `su` 與 `sudo` 活動也很重要，它們可以告訴你誰試圖以異常權限在活動。

經常檢視稽核軌跡可以讓你發現潛在的權限誤用狀況，以及系統上的其他異常活動。

關於記錄機制的進一步資訊，請查閱 <http://www.loganalysis.org/>

[回頁首 ^](#)

U4. 版本控制系統 (Version Control Systems)

U4.1 說明

版本控制系統所提供的工具可用以管理不同版本的文件與原始碼，並且幫助多使用者處理協同工作或共用檔案。這對於軟體發展專案、合作與法律文件的管理是不可或缺的，因為它們不只提供了中央儲存的方案，還允許回復至不同版本。

一致性版本維護系統 (CVS) 是今日 Linux/Unix 環境下最多人使用的原始碼版本控制系統。許多開放原始碼專案都允許匿名存取 CVS 儲藏區，而 CVS 儲藏區又可被設定為允許使用 `pserver` 協定遠端存取，預設使用 2401/tcp 連接埠。這樣可能造成下列弱點：

- A. 利用特製的 `Entry` 行可觸發堆積型的緩衝區溢位。攻擊者可利用緩衝區溢位在 CVS 伺服器上執行任意程式碼。針對 Linux、FreeBSD 與 Solaris 平台上 CVS 伺服器所寫的攻擊程式已被公布於安全郵件論壇。注意，所有被設定為可匿名存取的儲藏區都具有此弱點。
- B. 實作其他指令或函數時的弱點可被通過身分驗證的攻擊者利用，對 CVS 伺服器造成阻絕服務，或在 CVS 伺服器上執行任意程式。某些弱點還可被匿名使用者侵入。

Subversion 是另一個 Linux 上日益普及的版本控制系統，其目的是要設計出比 CVS 更好的系統。如果執行 `svnserve`，就可以使用 `svn` 協定存取 Subversion 儲藏區。`svn` 伺服器預設使用 3690/tcp 連接埠。這個伺服器包含了下列弱點：

- 未經身分驗證的使用者可利用堆積型的緩衝區溢位問題執行任意程式。

- 特製的 `get-dated-rev svn` 指令可觸發堆疊型的緩衝區溢位。若伺服器允許匿名存取，則可能讓未經身分驗證的攻擊者在伺服器上執行任何程式。網際網路上已有多個攻擊程式流傳。

如果攻擊者取得存取權限，他不但可以在原始碼中埋入後門或錯誤程式碼，讓開發軟體散布出去後形成廣大受害者群；還可以偽冒身分陷害其他善良使用者。

U4.2 受影響的作業系統：

Linux, FreeBSD, AIX, HP-UX, Solaris 與 SGI 及任何執行 CVS 或 Subversion 的系統。

U4.3 CVE/CAN 項目

[CAN-2004-0396](#), [CAN-2004-0414](#), [CAN-2004-0416](#), [CAN-2004-0417](#), [CAN-2004-0418](#), [CAN-2004-0397](#), [CAN-2004-0413](#)

U4.4 如何得知你是否具有弱點

如果你的 CVS 伺服器使用下列版本，且允許 `pserver` 協定進行遠端存取，則你的伺服器具有弱點：

- CVS stable release 1.11.16 之前版本
- CVS feature release 1.12.8 之前版本
- 可使用 `cvsversion` 指令查詢 CVS 版本。

如果你的 Subversion 伺服器使用 1.0.5 之前版本，且允許 `svn` 協定進行遠端存取，則你的伺服器具有弱點。

U4.5 如何針對弱點進行防護

針對 CVS Server：

- 確保 CVS 軟體具有最新修補等級。新版軟體原始碼可由此下載：<https://www.cvshome.org/>.
- 使用 SSH 協定替代 `pserver` 協定進行遠端存取。另外，使用 `chroot` 環境執行 CVS 伺服器。詳細作法請參閱：<http://www.netsys.com/library/papers/chrooted-ssh-cvs-server.txt>
- 如果 CVS 儲藏區可由公司內網存取，請網路邊境上阻擋 2401/tcp 連接埠。
- 確認所有公布的攻擊程式都無法入侵你的 CVS 伺服器，這些程式可在這裏找到：
http://www.k-otik.com/exploits/05212004.CVS_Linux.c.php http://www.k-otik.com/exploits/05212004.CVS_Solaris.c.php
- CVS 伺服器只應允許匿名者擁有讀取權限，並安裝於獨立系統環境，例如 DMZ。

針對 Subversion Server：

- 確保 Subversion 伺服器更新到最新版本。最新版本可由此下載：<http://subversion.tigris.org>
- 設定 Subversion 儲藏區，使用 webDAV 協定替代 `svn` 協定進行遠端存取。
- 如果 Subversion 儲藏區可由公司內網存取，請網路邊境上阻擋 3690/tcp 連接埠。
- 確認所有公布的攻擊程式都無法入侵你的 Subversion 伺服器，這些程式可在這裏找到：
http://www.metasploit.com/projects/Framework/modules/exploits/svnserve_date.pm
<http://www.k-otik.com/exploits/06112004.subexp.c.php>
- Subversion 伺服器只應允許匿名者擁有讀取權限，並安裝於獨立系統環境，例如 DMZ。

U4.6 參考資料

CERT 通報

<http://www.kb.cert.org/vuls/id/192038>

SecurityFocus BIDs

<http://www.securityfocus.com/bid/10384> <http://www.securityfocus.com/bid/10499>
<http://www.securityfocus.com/bid/10386> <http://www.securityfocus.com/bid/10519>

CVS 首頁

<http://www.cvshome.org>

Subversion 首頁

<http://subversion.tigris.org>

安全文章列表

<http://www.securityfocus.com/archive/1/363775/2004-05-17/2004-05-23/0>
<http://www.securityfocus.com/archive/1/365541/2004-06-07/2004-06-13/0>
<http://www.securityfocus.com/archive/1/363781/2004-05-17/2004-05-23/0>
<http://archives.neohapsis.com/archives/bugtraq/2004-06/0180.html>

[回頁首 ^](#)

U5. 郵件傳送服務(Mail Transport Service)

U5.1 說明

電子郵件是網際網路上最廣為使用的服務之一，而 SMTP 則是最老的通訊協定之一。郵件轉送代理伺服器(MTA)負責由送件端取得信件，再送給收件端，通常使用 SMTP 協定。只要寄件端與收件端同時支援，SMTP 協定就可為不安全的埠號加上 TLS 以使用 SSL 加密。Sendmail 是頗為普及的 Unix 平台 MTA，但在經過長年安全質疑及過於複雜的設定下，幾個大受歡迎的替代軟體逐漸崛起，包括 Qmail、Courier-MTA、Postfix 與 Exim。

在電子郵件如此普及的今日，郵件系統會被病毒、網蟲及攻擊者不斷攻擊並不讓人意外。雖然許多攻擊都是針對常用的郵件用戶端軟體，但 MTA 也是誘人的目標。伺服器弱點所引起的威脅可分為下面幾類：

- 攻擊未修補的系統，包含緩衝區溢位、堆積溢位等。
- 濫用開放轉發(open relay)功能，垃圾郵件業者的最愛。
- 利用其他非轉發的錯誤設定，像是使用者帳號資料庫可用於寄送垃圾郵件或進行社交工程攻擊（或電子郵件用戶攻擊）。

如果網路上存在具有弱點的 MTA，保證馬上會被發現並入侵。所幸你可以在安裝或進行定期基本維護時，藉由幾個簡單步驟來有效降低風險。遵循 RFC 來實作的 MTA 是最好的選擇，而多數垃圾信件軟體並不這麼作。

U5.2 受影響的作業系統：

幾乎所有 Unix 類的主機都附有上述的 MTA 之一。雖然近年來大多數 Unix 廠商都改善了預設安裝時的安全，未修補、未維護、或在預設設定下執行的 MTA 仍應被視為具有弱點。

U5.3 CVE/CAN 項目

Sendmail

[CVE-1999-0047](#), [CVE-1999-0095](#), [CVE-1999-0096](#), [CVE-1999-0129](#), [CVE-1999-0131](#), [CVE-1999-0203](#),
[CVE-1999-0204](#), [CVE-1999-0206](#), [CVE-1999-1109](#), [CVE-2000-0319](#), [CVE-2001-0653](#), [CVE-2001-1349](#),
[CVE-2002-0906](#)

[CAN-1999-0098](#), [CAN-1999-0163](#), [CAN-2001-0713](#), [CAN-2001-0714](#), [CAN-2001-0715](#), [CAN-2002-1165](#),
[CAN-2002-1278](#), [CAN-2002-1337](#), [CAN-2003-0161](#), [CAN-2003-0285](#), [CAN-2003-0694](#)

Qmail

[CVE-2000-0990](#), [CAN-2003-0654](#)

Courier-MTA

[CVE-2002-0914](#), [CVE-2002-1311](#), [CVE-2003-0040](#), [CVE-2004-0224](#), [CVE-2004-0777](#)

Exim

[CVE-2001-0889](#)

[CAN-2003-0743](#), [CAN-2004-0399](#), [CAN-2004-0400](#)

Postfix

[CAN-2003-0468](#)

U5.4 如何得知你是否具有弱點

- **檢查修補等級**

要知道你的系統是否具有弱點，第一步就是檢查現用 MTA 的修補等級，並找出該版本是否具有弱點。利用 CVE (<http://cve.mitre.org/>) 可以讓你知道你的 MTA 具有哪些相關弱點。

Sendmail

Sendmail 過去曾被發現非常多弱點，多半歸因於它的複雜性。這使得 Sendmail 成為網際網路上最常被侵害的系統之一。

任何未更新或未修補的版本都可能具有弱點。

想知道 Sendmail 的版本，請鍵入下列指令：

```
echo \[extract_itex] | sendmail -bt -d
```

不要絕對相信服務程式回傳的版本結果，因為它是讀取某個文字檔案中的記錄，而該文字檔可能並未正常更新。

要知道最新版本為何，請查閱 Sendmail 網站：<http://www.sendmail.org/current-release.html>

Exim

Exim 是另一套頗受歡迎的全功能 MTA。它曾被發現幾個弱點。

想知道 Exim 的版本，請鍵入下列指令：

```
exim -bV
```

要知道最新版本為何，請查閱 Exim 網站：<http://www.exim.org/version.html>

Qmail

Qmail 是以安全為導向的 MTA，但也曾發現具有幾個弱點。它也是 Sendmail 之後最受歡迎的 MTA 之一。

沒有簡單可靠的方法可以找出 Qmail 版本，只能使用 GUN grep 指令由 man 說明中猜測：

```
grep -A1 version /var/qmail/man/man7/qmail.7
```

Qmail 有許多使用者貢獻的增強功能，讓辨識出弱點的工作更為複雜。

你可以在這裏找到 Qmail 的建議修補程式：<http://www.qmail.org/top.html#patches>，也可以在這裏找到將 qmail 和建議修補程式一起包裝而成的套件（稱為 netqmail）：
<http://www.qmail.org/netqmail/>

Courier-MTA

Courier-MTA 是一個嚴格依循 RFC 所開發的郵件伺服器，支援 Maildir+、maildrop、MySQL、Postgresql 及 LDAP，提供別名與儲存使用者帳號的功能。

想要知道你現用的版本，請使用 `showmodules` 指令。

要得知 安全通知與最新版本，請造訪：<http://www.courier-mta.org>

Postfix

一如 Qmail，Postfix 是以安全為導向的 MTA，但被發現的弱點更少。最新版增加了存取控制、內容審視及送件率限制等加強功能。雖然現有版本可能沒有弱點，最好還是更新到新版。

想要知道你現用的 Postfix 版本，請鍵入下列指令：
`postconf -d mail_version`

要知道最新版本為何，請查閱 Postfix 網站：<ftp://ftp.porcupine.org/mirrors/postfix-release/index.html>

- **檢查轉發狀態**

什麼是開放轉發(open relay)

信件轉發是 MTA 的基本功能。不良的設定會讓 MTA 變為開放轉發狀態，造成 MTA 不管寄件者或收件者是否為本機使用者，都直接轉發郵件訊息。換句話說，郵件傳送過程中的寄件端或收件端都不是自身網域或 MTA 的一部分。正常情形下這種郵件不應經過 MTA。

檢查你的 MTA 是否為開放轉發

檢查 MTA 是否為開放轉發，是在安裝完修補程式後頭一件要作的事。這可以讓你知悉 MTA 是否會被人利用來寄送垃圾郵件。下列工具可以協助進行檢查：

<http://www.abuse.net/relay.html>

<http://www.cymru.com/Documents/auditing-with-expect.html>

什麼是即時黑名單？

即時黑名單 (RBL) 是一份 IP 位址清單，列出了所有拒絕協助阻止垃圾郵件擴散的管理者所負責的伺服器。郵件管理者可以依據這份清單來拒絕這些伺服器對 MTA 的連線，以防範已知的垃圾郵件業者。

找出你的郵件伺服器是否被列入 RBL

如果你發現你的郵件伺服器名列榜上，可能是因為開放轉發所造成，除非你最近調整過伺服器。你的使用者濫用伺服器散發垃圾郵件或電子報也會讓你被列入 RBL。你可以到這裏來找看看有沒有你伺服器的 ip：

<http://www.mail-abuse.com/support/lookup.html>

<http://www.ordb.org/>

不過要注意，RBL 裏的位址太多了，這個網頁只列出最常見的幾個。

- **稽核郵件伺服器**

稽核你的郵件伺服器讓你可以找出會被惡意使用者利用的弱點，以防他們利用你的郵件伺服器進行未經授權的活動。

Nessus

Nessus 是一個免費且強大的弱點掃描軟體，它含有一些 SMTP 伺服器的專屬插件。這可以讓你快速有效地辨識出 MTA 弱點。

你可以在此找到 Nessus 及相關插件：<http://www.nessus.org>

SARA

Sara 為 Security Auditor's Research Assistant 的縮寫，是一個安全分析工具，可以掃描包含 SANS 首廿大清單在內的弱點。

SARA 可在這裏找到：<http://www-arc.com/sara/>

U5.5 如何針對弱點進行防護

請採取下列步驟來保護你的郵件伺服器，這些步驟分為兩部分。一般建議裏列出的是與郵件伺服器產品無關的建議，而專屬建議裏則針對 Sendmail、Qmail 與 Postfix 郵件伺服器列出相關建議：

1. 一般建議

- 確認是否需要使用 MTA，以及 MTA 是否需要公開服務
- 停用系統上任何未經許可或特別指定使用的郵件服務，並制定流程以防它被再度啓用。在防火牆上套用相關的強制規制。
- 套用廠商修補程式，或更新郵件伺服器到最新版本。
- 使用獨立的內部 MTA 來處理內部郵件。
- 限制 MTA 執行的權限層級，可能的話，在 chroot 環境下執行。
- 閱讀有關郵件伺服器的所有文件，訂閱相關的郵件論壇。

預防信件轉發

要避免郵件伺服器被垃圾信件業者濫用，應設定不轉發由非信任網路或網域來的信件：

Sendmail

如果你必需以常駐程式(daemon)模式執行 Sendmail，必需確保它只轉發來自所管轄系統內的相關郵件，請參閱 <http://www.sendmail.org/tips/relaying.html> 與 http://www.sendmail.org/m4/anti_spam.html 來幫助你正確設定伺服器。從 8.9.0 版開始，開放轉發的功能已被預設停用。然而許多作業系統廠商均預設將它重新啓用。如果你使用的 Sendmail 是隨附於作業系統的版本，請特別注意確保伺服器未被設為轉發狀態。

Qmail

Qmail 提供了不錯的文件來討論選擇性轉發的問題，並幫助你停用系統的轉發功能。請參閱：<http://www.lifewithqmail.org/lwq.html#relaying>

Courier-MTA

預設使用封閉轉發，Courier 已提供文件來說明如何針對特定網路或 IP 位址啓用轉發功能。此外，它還可以使用 SMTP 身分驗證方式來提供轉發服務：
<http://www.courier-mta.org> FAQ section.

Exim

Exim 也有詳細文件說明如何預防轉發：
<http://www.exim.org/howto/relay.html>

Postfix

對 Postfix 來說，有一些步驟可以協助限制存取與轉發控制。只接受列於「mynetworks」參

數內主機或網路的轉發要求。請參閱：

http://www.postfix.org/SMTDPD_ACCESS_README.html

2. 其它與應用程式相關的細節

- A. 關於如何以更為安全的方式設定與執行 Sendmail，可參閱：
<http://www.sendmail.org/secure-install.html>
http://www.sendmail.org/m4/security_notes.html
<http://www.sendmail.org/~gshapiro/security.pdf>
- B. 要預防 Postfix 被入侵後佔領整個系統，可對其設限，以非特權帳號執行於 chroot() 目錄下。Postfix 的設定請參閱：
<http://www.linuxjournal.com/article.php?sid=4241>
- C. 這個連結以範例告訴你如何設定 MTA 使用黑名單：
<http://www.ordb.org/faq/#usage>
- D. Courier-MTA 預設就支援 RBL 名單，並在 esmtpd 的設定檔中提供了一個初始 rbl 伺服器清單。

Postfix 包含了一些可限制 UCE 的功能，相關資訊可由此取得：

<http://www.securitysage.com/antispam/intro.html>

[回頁首 ^](#)

U6. 簡單網路管理協定(Simple Network Management Protocol, SNMP)

U6.1 說明

簡單網路管理協定 (SNMP) 被廣泛用於遠端監控與設定管理，幾乎當今所有啓用 TCP/IP 的裝置都可適用。網路設備中處處可見 SNMP，它最常被使用於管理設定印表機、路由器、交換器、無線基地台，並為網路監控設備提供資料。

網路設備使用被稱為代理程式的軟體與 SNMP 管理站進行通訊，簡單網路管理的通訊包含了幾種不同交換訊息。處理這些訊息的方式、以及訊息處理背後的身分驗證機制都具有可被入侵的重大弱點。

因為 SNMP 一版處理及捕捉訊息的方式所造成的弱點細節可參閱 [CERT 通報 CA-2002-03](#)。管理站與代理程式在解析並處理捕捉(trap)及要求訊息時，曾經被發現有一些弱點。

這些弱點不只出現在 SNMP 本身的實作上，還同時影響到各家廠商整合 SNMP 功能後的分支產品。攻擊成功可以導致各種結果，從造成阻絕服務到修改設定，甚至接管你的 SNMP 設備

舊版 SNMP 架構中的身分驗證機制也有重大弱點。SNMP 一版和二版使用未加密的「社群字串 (community string, 或稱為社群名稱)」作為唯一的驗證機制。缺乏加密已經夠糟糕了，絕大多數 SNMP 裝置還都使用相同的預設社群字串「public」，只有少數明智的網路設備廠商會在需要提供進一步敏感資訊時改成「private」。攻擊者可以利用這項 SNMP 弱點由遠端重新設定或關閉裝置。竊聽 SNMP 封包則可對網路架構、設備與主機布署狀況一覽無遺。入侵者使用這些資訊來選擇目標並策劃攻擊。

大多數廠商預設啓用 SNMP 一版，且多半不提供 SNMP 三版安全模型的功能，亦即無法使用進階的身分驗證模式。然而在 GPL 或 BSD 授權下有一些免費替代軟體可以提供 SNMPv3 支援。

不只 UNIX，SNMP 也被廣泛使用於 Windows、網路設備、無線基地台與橋接器、印表機或嵌入式裝置。但是相關攻擊主要還是出現在 SNMP 設定不良的 UNIX 系統上。SNMP 在網路上以明文傳輸，因此在可監控環境下更應仔細考慮是否使用。

要知道更多與 SNMP 弱點相關的資訊，CERT CC 提供了一份 SNMP 常見問答集，可造訪：

http://www.cert.org/tech_tips/snmp_faq.html.

U6.2 受影響的作業系統：

幾乎所有 UNIX 與 Linux 系統都附加安裝了 SNMP，並通常預設啟用。啟用 SNMP 的其它網路設備與作業系統也大多數具有弱點。

U6.3 CVE/CAN 項目

CVE-1999-0294, CVE-1999-0472, CVE-1999-0815, CVE-1999-1335, CVE-2000-0221, CVE-2000-0379, CVE-2000-0515, CVE-2000-1058, CVE-2001-0236, CVE-2001-0487, CVE-2001-0514, CVE-2001-0564, CVE-2001-0888, CVE-2002-0017, CVE-2002-0069, CVE-2002-0302, CAN-1999-0186, CAN-1999-0254, CAN-1999-0499, CAN-1999-0516, CAN-1999-0517, CAN-1999-0615, CAN-1999-0792, CAN-1999-1042, CAN-1999-1126, CAN-1999-1245, CAN-1999-1460, CAN-1999-1513, CAN-2000-0147, CAN-2000-0885, CAN-2000-0955, CAN-2000-1157, CAN-2000-1192, CAN-2001-0046, CAN-2001-0352, CAN-2001-0380, CAN-2001-0470, CAN-2001-0552, CAN-2001-0566, CAN-2001-0711, CAN-2001-0840, CAN-2001-1210, CAN-2001-1220, CAN-2001-1221, CAN-2001-1262, CAN-2002-0012, CAN-2002-0013, CAN-2002-0053, CAN-2002-0109, CAN-2002-0305, CAN-2002-0478, CAN-2002-0540, CAN-2002-0812, CAN-2002-1048, CAN-2002-1170, CAN-2002-1408, CAN-2002-1426, CAN-2002-1448, CAN-2002-1555, CAN-2003-0137, CAN-2003-0935, CAN-2003-1002, CAN-2004-0311, CAN-2004-0312, CAN-2004-0576, CAN-2004-0616, CAN-2004-0635, CAN-2004-0714

U6.4 如何得知你是否具有弱點

你可以使用掃描軟體，或手動檢查網路連接裝置上是否啟用 SNMP。

- SNMPing – 可由 SANS 協會免費下載 SNMPing 掃描工具：<http://www.sans.org/alerts/snmp/>.
- SNScan – Foundstone 寫了另一隻易用的 SNMP 掃描工具，叫作 SNScan，可由此下載：http://www.foundstone.com/knowledge/free_tools.html.
- Nessus – 一個開放原始碼的安全評估掃描軟體，可在這裏找到：<http://www.nessus.org>

如果你不能使用上述工具，就得手動檢查系統上是否使用 SNMP，請參考相關的作業系統手冊以得知其 SNMP 實作方式。不過若使用 grep 指令在行程(process)列表中找尋「snmp」，通常可找到其基本常駐程式(daemon)；或也可直接找尋使用 161、162 埠號的程式（lsof 工具在找尋埠號及行程之間對應關係時十分有用）。

發現執行中的 SNMP 實體，可能就代表了你具有弱點，在處理捕捉或要求訊息時會發生錯誤。請參閱 [CERT 通報 CA-2002-03](#) 以得知進一步資訊。

如果 SNMP 執行時的參數符合下列情形，你就可能具有預設或易猜字串弱點：

1. 空白或預設的 SNMP 社群名稱。
2. 易猜的 SNMP 社群名稱。
3. 隱藏的 SNMP 社群名稱。

請參閱 <http://www.sans.org/resources/idfaq/snmp.php> 以瞭解如何辨別是否具有上述問題。

U6.5 如何針對弱點進行防護

處理捕捉與要求訊息時的弱點：

1. 如果沒有使用 SNMP 的必要，建議停用。
2. 儘可能配置 SNMPv3 安全模型，以使用訊息驗證，或為通訊協定資料單元進行加密。
3. 如果必須使用 SNMPv1 或 v2，請確定已更新廠商最新修補程式。第一步可從找出廠商相關資訊開始，請參閱 [CERT 通報 CA-2002-03](#) 的附錄 A。

4. 在對內的網路節點上過濾 SNMP(TCP/UDP 埠號 162 與 162)封包，除非你的裝置需要由外網進行管理。
5. 在使用 SNMP 代理程式的設備或系統上加上主機端存取控制。如果受限於作業系統本身功能，也可以改為控制代理程式該接受哪些系統要求。在多數 UNIX 系統上，可以使用 TCP-Wrappers 或設定 Xinetd 來達成。可針對代理程式進行封包過濾的本機防火牆亦可用於阻擋不請自來的 SNMP 要求。

預設及易猜字串弱點：

1. 如果沒有使用 SNMP 的必要，建議停用。
2. 儘可能配置 SNMPv3 安全模型，以使用訊息驗證，或為通訊協定資料單元進行加密。
3. 如果必須使用 SNMPv1 或 v2，使用密碼政策來規範社群名稱，確保它們難以被猜得或破解，並定期更換。
4. 用 snmpwalk 來檢驗社群名稱，參閱 <http://www.zend.com/manual/function.snmpwalk.php>。這裏有個不錯的教學範例：<http://www.sans.org/resources/idfaq/snmp.php>
5. 在對內的網路節點上過濾 SNMP(TCP/UDP 埠號 162 與 162)封包，除非你的裝置需要由外網進行管理。可能話，只允許可信任子網間的 SNMP 傳輸。

將 MIB 設為唯讀，進一步資訊請參閱：

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315

[回頁首 ^](#)

U7. 開放式安全傳輸層協定(Open Secure Sockets Layer, SSL)

U7.1 說明

開放原始碼 [OpenSSL](#) 函式庫為網路溝程式提供密碼學支援。它被許多廠商使用於 SSL/TLS 協定的實作，最有名的例子就是 Apache 網頁伺服器（支援 http 安全連線）。其他的應用實例還包含 POP3、IMAP、SMTP 與 LDAP 伺服器，它們都應用 OpenSSL 設計了類似的保護機制。

OpenSSL 函式庫被整合在許多程式中，所以可以透過這些程式來利用它的弱點。舉例來說，許多公開的攻擊程式針對的就是使用各版本 OpenSSL 函式庫編譯而成的 Apache 伺服器。然而同一支攻擊程式經過修改後，也可用於入侵 sendmail、openLDAP、CUPS 或其他應用 OpenSSL 的程式。

OpenSSL 函式庫曾被發現多個弱點。最嚴重的一次是 5 個弱點的集合，列於 CAN-2002-0655、CAN-2002-0656、CAN-2002-0557、CAN-2002-0659 與 CAN-2003-0545。這些弱點可被遠端侵入，利用 OpenSSL 函式庫相關程式的權限執行任意程式。在多數情形下（例如 sendmail），攻擊成功都可奪得 root 權限。

U7.2 受影響的作業系統：

所有使用下列 OpenSSL 版本的 UNIX 或 LINUX 系統都會受影響：(a) 0.9.7c 或之前版本(b) 0.9.6l 或之前版本。這也影響到 Linux 配布套件軟體，像是 Apache、CUPS、Curl、OpenLDAP、Stunnel、Sendmail 與其他應用 OpenSSL 的程式。

U7.3 CVE/CAN 項目

[CVE-1999-0428](#), [CVE-2001-1141](#), [CAN-2000-0535](#), [CAN-2002-0655](#), [CAN-2002-0656](#), [CAN-2002-0557](#), [CAN-2002-0659](#), [CAN-2003-0078](#), [CAN-2003-0131](#), [CAN-2003-0147](#), [CAN-2003-0543](#), [CAN-2003-0544](#), [CAN-2003-0545](#), [CAN-2003-0851](#), [CAN-2004-0079](#), [CAN-2004-0081](#), [CAN-2004-0112](#), [CAN-2004-0607](#)

U7.4 如何得知你是否具有弱點

檢查「openssl version」指令的結果。如果版本不是 0.9.7d 或 0.9.6m，則系統具有弱點。

U7.5 如何針對弱點進行防護

1. 更新 OpenSSL 到最新版本。如果是作業系統隨附安裝的版本，請更新廠商提供的最新修補程式。注意，更新過程中有時會需要重新編譯或重新連結程式。

還有個彈性作法，你可以使用 `ipfilter` / `netfilter` 或其他具有防火牆功能的工具，限制系統對有啓用 OpenSSL 的伺服器進行連接。注意，因為 OpenSSL 被廣為用於保護對網際網路上電子商務的 HTTP 活動，所以這樣的主機限制可能不合用。

[回頁首 ^](#)

U8. 企業服務 NIS/NFS 的錯誤設定 (Misconfiguration of Enterprise Services NIS/NFS)

U8.1 說明

網路檔案系統(NFS)與網路資訊服務(NIS)是常用於 UNIX 伺服器與網路上的兩個重要服務。NFS 是 Sun Microsystems 提出的服務，被設計用來讓網路上的 UNIX 系統彼此分享（匯出）檔案系統、目錄或檔案。NIS 則是一群以鬆散分散式資料庫形式提供的服務程式，用以將位址資訊（稱為地圖）提供給其他網路服務，網路檔案系統(NFS)就是其中一種。最常被製成地圖的資訊是 `passwd` 與 `group` 檔的連結，好讓集中式的使用者身份驗證機制使用。`host` 檔亦是 NIS 的常用目標。

近年來，這兩種服務程式上的安全問題不斷浮現（緩衝區溢位、阻絕服務、不良身分驗證），使得他們成為攻擊活動經常選用的目標。

除了未修補的服務程式遍及四處之外，更大的風險來自於對 NFS 與 NIS 的設定不當，這使得它們被遠端或本機使用者輕易入侵。

使用者可使用 `ypcat` 或 `getent` 等程式來查詢並顯示 NIS 資料庫或地圖資料，但 NIS 提供的馬虎身分驗證機制卻讓這些工具可以擷取到密碼檔。同樣問題也發生在 NFS 上，它無條件信任 NFS 用戶端提供、或在伺服器設定中所指定的 UID(使用者 ID)與 GID(群組 ID)，讓任何使用者都可掛載或瀏覽遠端檔案系統。

U8.2 受影響的作業系統：

幾乎所有 UNIX 與 Linux 系統都隨附 NFS 與 NIS，並通常預設啓用。NFS 雖然預設啓用，但其匯出檔（用以指明分享目錄及分享方式）通常為空檔案。

U8.3 CVE/CAN 項目

NFS

[CVE-1999-0002](#), [CVE-1999-0166](#), [CVE-1999-0167](#), [CVE-1999-0170](#), [CVE-1999-0211](#), [CVE-1999-0832](#), [CVE-1999-1021](#), [CVE-2000-0344](#), [CVE-2002-0830](#)

[CAN-1999-0165](#), [CAN-1999-0169](#), [CAN-2000-0800](#), [CAN-2002-0830](#), [CAN-2002-1228](#), [CAN-2003-0252](#), [CAN-2003-0379](#), [CAN-2003-0576](#), [CAN-2003-0680](#), [CAN-2003-0683](#), [CAN-2003-0976](#), [CAN-2004-0154](#)

NIS

[CVE-1999-0008](#), [CVE-1999-0208](#), [CVE-1999-0245](#), [CVE-2000-1040](#)

[CAN-1999-0795](#), [CAN-2002-1232](#), [CAN-2003-0176](#), [CAN-2003-0251](#)

U8.4 如何得知你是否具有弱點

下列步驟可檢查 NIS/NFS 軟體弱點：

1. 檢查廠商所釋出的最新版本。多半經由 `rpc.mountd` 指令來檢查 NFS 版本，及用 `ypserv` 檢查 NIS 版本。任何未修補或舊版都可能具有弱點。
2. 針對軟體弱點而言，比較完整的作法是使用更新後的弱點掃描軟體，定期檢查你的系統是否具有新的漏洞。

下列步驟用於檢查 NIS 設定：

1. 確保 NIS 地圖中不包含 root 密碼。
2. 檢查使用者密碼是否符合標準安全規範，可利用密碼破解器來達成。
3. 如果可能的話，密碼雜湊使用 Blowfish 或 MD5 來代替 DES。

特別注意：若無長官允許，絕對不要使用任何密碼破解器，即使是針對你有管理權限的系統。許多好心的管理者因為未經授權執行密碼破解器而被開除。

下列步驟用於檢查 NFS 設定：

1. 確認 `/etc/exports` 檔案中的主機、網路群組與權限等設定項目是否保持更新。
2. 執行「`showmount -e 伺服器 IP`」指令來檢查匯出了哪些資源。檢查掛載資源是否符合安全政策。

U8.5 如何針對弱點進行防護

下列步驟用於檢查 NIS 設定：

1. 在用戶端指定可連結之 NIS 伺服器，以防網路上偽冒的 NIS 伺服器。
2. 製作 DBM 檔案時，啟用 `YP_SECURE` 功能以確保伺服器只回應來自特權埠號的用戶端。可使用 `makedbm` 指令的 `s` 參數達成。
3. 在 `ypserv` 與 `ypxfrd` 所使用的 `/var/yp/securenets` 檔中加入可信任的主機與網路，請記得要重新啟動常駐程式(`dameon`)才能使設定生效。
4. 確認 NIS 用戶端的密碼檔中具有「`+:*:0:0:::`」這行。
5. 考慮在安全協定下使用 NIS，例如 SSH。可由此開始：
<http://www.math.ualberta.ca/imaging/snfs/>.

注意：某些設定已使用輕量目錄存取協定(LDAP)來取代 NIS。所有 Linux 版本都支援將 LDAP 作為名稱服務元件的來源，像是 `passwd`、`group` 與 `hosts`。一本好的 LDAP 系統管理手冊會十分有用。此外，LDAP 天生就支援複製及 SSL 加密功能。

下列步驟用於檢查 NFS 設定：

1. 在 `/etc/exports` 中設定允許用戶端時，避免採用 `hosts` 檔或 NIS `hosts` 地圖中的別名，請採用數字 IP 或完整的網域名稱。
2. 在 `/etc/exports` 檔中利用下列參數來限制 NFS 檔案系統的存取權限：
 - 要防止普通使用者掛載 NFS 檔案系統，請在 `/etc/exports` 檔中 NIS 用戶端的 IP 位址或網域名稱後加上 `secure` 參數。
(例：`/home 10.20.1.25(secure)`)。
 - 以適當的權限匯出 NFS 檔案系統。請在 `/etc/exports` 檔中 NIS 用戶端 IP 位址或網域名稱後加上權限 (`ro` 代表唯讀、`rw` 代表可讀

寫)。

(例：/home 10.20.1.25(ro))。

- 可能的話，在/etc/exports 檔中 NTS 用戶端 IP 位址或網域名稱後加上 root_squash 參數。啓用這個參數後，NFS 用戶端上的超級使用者 ID root 就會被 NTF 伺服器上的使用者 ID nobody 與群組 ID nobody 所取代（可修改 anonuid 與 anongid 以指定所需 ID）。這表示對於伺服器端 root 使用者可存取或修改的檔案，用戶端 root 使用者無法進行存取或修改，以預防它取得伺服器特權。

(例：/home 10.20.1.25(root_squash))

- 如果你要使用匿名權限匯出目錄，請使用「all_squash」參數，這可以將所有使用者 id 及群組 id 對應到 anonuid 與 anongid ID。
- 完整的參數設定可在/etc/exports 的 man 說明頁中找到。請使用「man exports」指令，或線上說明：

<http://www.netadmintools.com/html/5exports.man.html>

3. 有個叫作 NFSBug 的工具可用來檢測設定值。測試項目中包含了找出系統上所有匯出的檔案系統、檢查所有匯出限制是否有效、檢查檔案系統是否可透過 portmapper 來掛載、試著猜解檔案處理號(file handle)、及試著利用各種程式錯誤來存取檔案系統。

<http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/nfsbug/>

4. 在 Solaris 上需確認啓用埠號監控功能，請將「set nfssrv:nfs_portmon = 1」這行加入 /etc/system 檔中。Linux 系統預設拒絕 NFS 用戶端使用非特權（超過 1024）埠號。

一般對 NIS 與 NFS 的考量：

1. 檢視防火牆政策，確認是否已阻擋所有不需使用的埠號，包括 111/tcp/udp (Portmap) 及 2049/tcp/udp (Rpc.nfsd)連接埠。只允許核可的用戶端存取 NIS 與 NFS 伺服器。另一個可以用以限制的方式是透過 tcp_wrappers：
<http://sunsite.cnlab-switch.ch/ftp/software/security/security-porcupine.org/>.

在你的 /etc/hosts.allow 檔中明列可允許存取服務的服務程式與 IP（例：portmap: 10.20.0.0/16 可允許 Class-B 的私有網路 10.20.0.0 存取 portmap 服務），同時在 /etc/hosts.deny file 檔中明列不允許存取服務的服務程式與 IP（例：portmap: ALL 代表拒絕所有未列於/etc/hosts.allow 檔中的其他 IP 進行存取）。關閉對 portmap 服務的存取權限是很重要的，因為 NFS 透過它進行操作。

2. 考慮在安全協定下使用 NFS，例如 SSH。可由此開始：
<http://www.math.ualberta.ca/imaging/snfs/>.
3. 套用所有廠商的修補程式，或將 NIS 或 NFS 伺服器更新到最新版。關於進一步強化 UNIX 系統的資訊，請參閱 CERT 的 [UNIX 安全檢查清單](#)。

停用所有未認可成爲 NFS 或 NIS 伺服器系統上的 NFS 與 NIS 常駐程式(daemon)。要預防這項設定不被變更回來，比較聰明的作法就是將 NFS 與 NIS 軟體由系統上移除。

[回頁首 ^](#)

U9. 資料庫(Databases)

U9.1 說明

資料庫是電子商務、金融、銀行與企業資源管理(ERP)系統中的元素，其中包含了企業夥伴、客戶

與員工的重要資訊。資料庫管理系統是一群工具程式的集合，用以儲存、變更及粹取資料庫中的資訊。即使維持資料完整性與機密性是如此重要，對於資料庫管理系統(DBMS)的安全等級要求仍常常不及作業系統與網路。

多數企業與政府組織都使用資料庫來管理個人資訊，像是員工薪資、醫療記錄、過往經歷、貿易記錄、商場交易及會計資料。資料庫中亦會詳記客戶資訊，包含金融帳戶、信用卡號及企業夥伴的信任資料。但資料完整性與機密性會被許多方式破壞，包括複雜的實作、不安全的密碼、設定不當、不良程式碼、密碼儲存於程式碼中、以及未知的系統後門。

資料庫是極為複雜的應用程式，通常難以正確設定並進行保護。MySQL、PostgreSQL 與 ORACLE 等資料庫程式包含了許多功能：使用者帳號與密碼、密碼稽核系統、權限模型與為控制資料物件而指定的權限、內建指令、獨特的程式語法、網路協定、修補程式與服務套件、以及強大的資料庫管理能力與發展工具。許多管理者都是在閒暇之餘才處理資料庫管理事務，而且通常無法掌握如此複雜的應用程式，以致難以察覺嚴重的安全弱點與不當設定。傳統安全社群多半忽略資料庫安全議題，許多資料庫專家也未將安全視為己任。大部分資料庫都有一卡車的功能會被惡用或入侵，讓資料機密性、完整性與可獲得性受到侵害。

現代所有的關聯式資料庫系統都使用網路位址連接埠方式，意即任何擁有查詢工具的人都可直接連上資料庫而毋需透過作業系統的安全機制。舉例而言，Oracle 可透過 TCP 埠號 1521、MySQL 可透過 TCP 埠號 3306、PostgreSQL 可透過 TCP 埠號 5432 進行存取。大部分資料庫也具有公開的預設帳號密碼，並為資料庫資源與表格提供變化多端的存取方式。今日，多數資料庫都與前端應用程式緊密連結，最常見的就是網頁應用。如果應用程式本身或設定不良，則可讓攻擊者發動 SQL 注入攻擊，或利用某些資料庫弱點進行入侵。

CERT CC 發布了一份通報(CA-2003-05)，是有關數個可入侵後端 Oracle 資料庫的弱點。更近期的還有 US-CERT 發布的通報，談到 Oracle E-Business Suite 中的 SQL 注入弱點(TA04-160A) 可侵害資料庫程式與資料完整性。

同樣的，MySQL 也具有幾個弱點。對 MySQL 的常見攻擊簡述可參閱 Next Generation Software 近期發表的一篇論文：<http://www.nextgenss.com/papers/HackproofingMySQL.pdf>

U9.2 受影響的作業系統：

幾乎所有 Linux 系統都隨附開放原始碼 DBMS，像是 MySQL 或 PostgreSQL；還有一些商用的 DBMS 解決方案，像是 Oracle。各種 UNIX 平台，例如 Solaris、AIX 與 HP-UX 都支援 ORACLE、DB2、以及其他商用或開放原始碼 DBMS。

U9.3 CVE/CAN 項目

Oracle:

[CVE-2002-0567](#), [CVE-2002-0571](#)

[CAN-1999-0652](#), [CAN-1999-1256](#), [CAN-2002-0858](#), [CAN-2002-1264](#), [CAN-2003-0095](#), [CAN-2003-0096](#), [CAN-2003-0222](#), [CAN-2003-0634](#), [CAN-2003-0727](#), [CAN-2003-0894](#)

MySQL:

[CVE-1999-1188](#), [CVE-2000-0045](#), [CVE-2000-0148](#), [CVE-2000-0981](#), [CVE-2001-0407](#)

[CAN-1999-0652](#), [CAN-2001-1274](#), [CAN-2001-1275](#), [CAN-2002-0229](#), [CAN-2002-0969](#), [CAN-2002-1373](#), [CAN-2002-1374](#), [CAN-2002-1375](#), [CAN-2002-1376](#), [CAN-2003-0073](#), [CAN-2003-0150](#), [CAN-2003-0515](#), [CAN-2003-0780](#), [CAN-2004-0381](#), [CAN-2004-0388](#), [CAN-2004-0627](#), [CAN-2004-0628](#)

PostgreSQL:

[CVE-2002-0802](#)

CAN-1999-0862, CAN-2000-1199, CAN-2001-1379, CAN-2002-0972, CAN-2002-1397, CAN-2002-1398, CAN-2002-1399, CAN-2002-1400, CAN-2002-1401, CAN-2002-1402, CAN-2003-0040, CAN-2003-0500, CAN-2003-0515, CAN-2003-0901, CAN-2004-0366, CAN-2004-0547

U9.4 如何得知你是否具有弱點

確保隨附於作業系統的 DBMS 都使用最新版本。未修補、舊版資料庫都可能具有弱點。

使用 DBMS 預設安裝的話，就可能具有弱點可讓攻擊者入侵。

在系統上執行弱點掃描來檢查 DBMS 軟體是否具有弱點：

- **MySQL Network Scanner**：可掃描整個網路，找出使用預設（空白）密碼、及未經許可的 MySQL 伺服器。
- 開放原始碼掃描軟體 Nessus (<http://www.nessus.org>) 也具有檢查碼可檢查 UNIX 上常見的資料庫漏洞。
- 商用掃描軟體如 Foundstone、Qualys、eEye Retina 亦可偵測資料庫弱點。
- 除此之外還有些資料庫專屬掃描軟體，像是 AppSecInc 或 ISS Database Scanner。

U9.5 如何針對弱點進行防護

首先最重要的，確認資料庫程式是否安裝到最新修補等級。請由各廠商網站查詢修補資訊：

- Oracle (<http://otn.oracle.com/software/index.html>)
- MySQL (<http://www.mysql.com/products/mysql/>)
- PostgreSQL (<ftp://ftp.postgresql.org/pub>)

接下來確保 DBMS 與應用程式的 安全：

- 使用最小權限原則。
- 將系統部署到網路上前，移除或變更資料庫上特權或系統帳號的密碼。
- 儘可能使用預儲程序(stored procedure)。
- 移除或停用不需使用的預儲程序。
- 設定任何欄位格式的長度上限。
- 由伺服器端確認資料有效性（長度、格式、型態）。

可協助保護 DBMS 安全的幾個資源：

- Oracle (<http://otn.oracle.com/deploy/security/index.html>)
- MySQL (<http://dev.mysql.com/doc/mysql/en/Security.html>)
- PostgreSQL (<http://www.postgresql.org/docs/7/interactive/security.htm>)

追蹤廠商的弱點與安全通報：

- Oracle 安全通報：<http://otn.oracle.com/deploy/security/alerts.htm>)
- MySQL (<http://lists.mysql.com/>)
- PostgreSQL (<http://www.postgresql.org/lists.html>)

SANS 協會發布了一份 Oracle 安全檢查清單，在稽核 Oracle 資料庫程式方面十分有用：
<http://www.sans.org/score/oraclechecklist.php>

The Center for Internet Security 發展了一套 Oracle 資料庫評量工具，對於量測資料庫安全性也很有用：http://www.cisecurity.org/bench_oracle.html

SANS〈一步步保護 Oracle 安全〉提供了許多實用的 Oracle 強化技巧 (https://store.sans.org/store_item.php?item=80)

可由下列網址查閱進一步資訊：

- SANS 讀書間關於資料庫安全的部分 (http://www.sans.org/rr/catindex.php?cat_id=3)
- <http://www.petefinnigan.com/orasec.htm>

[回頁首 ^](#)

U10. 系統核心(Kernel)

U10.1 說明

作業系統的中樞就是系統核心。系統核心負責作業系統與硬體、記憶體、排程、內部程序通訊、檔案系統及其他元件間的溝通。因為系統核心具有系統上所有物件的存取權限，核心層級的入侵可能會導致大崩毀。核心弱點造成的風險包含了阻絕服務(Denial of service)、使用系統權限執行任意程式、不受限制地存取檔案系統、或取得管理者等級權限。許多弱點都可經由遠端入侵，尤其是透過公開於網際網路上的服務。在某些情形下，送出特製的 icmp 封包就可讓系統核心進入執行迴圈，耗盡 CPU 資源使得系統無法正常運作，造成阻絕服務狀態。

適當地調整系統核心不只可以保護系統免受攻擊，還可增進系統效能。

U10.2 受影響的作業系統：

幾乎所有繼承 UNIX 概念的系統，包含 Solaris、HP-UX、Linux 各種發行版本、BSD 版及 Windows 版都曾具有核心弱點，這些弱點有些是由繼承而來，有些是被應用程式弱點所影響。

U10.3 CVE/CAN 項目

[CVE-1999-0295](#), [CVE-1999-0367](#), [CVE-1999-0482](#), [CVE-1999-0727](#), [CVE-1999-0804](#), [CVE-1999-1214](#), [CVE-1999-1339](#), [CVE-1999-1341](#), [CVE-2000-0274](#), [CVE-2000-0375](#), [CVE-2000-0456](#), [CVE-2000-0506](#), [CVE-2000-0867](#), [CVE-2001-0062](#), [CVE-2001-0268](#), [CVE-2001-0316](#), [CVE-2001-0317](#), [CVE-2001-0859](#), [CVE-2001-0993](#), [CVE-2001-1166](#), [CVE-2002-0046](#), [CVE-2002-0766](#), [CVE-2002-0831](#)

[CAN-1999-1166](#), [CAN-2000-0227](#), [CAN-2001-0907](#), [CAN-2001-0914](#), [CAN-2001-1133](#), [CAN-2001-1181](#), [CAN-2002-0279](#), [CAN-2002-0973](#), [CAN-2003-0127](#), [CAN-2003-0247](#), [CAN-2003-0248](#), [CAN-2003-0418](#), [CAN-2003-0465](#), [CAN-2003-0955](#), [CAN-2003-0984](#), [CAN-2004-0003](#), [CAN-2004-0010](#), [CAN-2004-0177](#), [CAN-2004-0482](#), [CAN-2004-0495](#), [CAN-2004-0496](#), [CAN-2004-0497](#), [CAN-2004-0554](#), [CAN-2004-0602](#)

U10.4 如何得知你是否具有弱點

有幾種方法可讓你檢查系統核心否具有弱點：

- 如果作業系統由廠商所提供，請在進行軟體註冊時，同時註冊安全更新通知服務。
- 多數以安全為主題的郵件論壇(Mailing List)都會在收到通知後即時公布核心弱點。
- 追蹤系統核心版本，並列為標準作業流程。
- 弱點評估軟體可用以找出系統核心版本。Nessus 具有許多插件可用以檢測核心弱點。注意，其中一些插件可能會造成阻絕服務，掃描時需十分謹慎以免發生未預警的當機。

U10.5 如何針對弱點進行防護

有兩類核心參數可供調整以預防攻擊。一種是調整所耗用的系統資源，以限制阻絕服務與緩衝區溢

位。第二種是強化網路設定以預防網路攻擊。所需使用的指令與參數依作業平台而異，請詳讀各作業平台文件，以瞭解如何妥當地調整系統核心。

我們建議要對正在運作的主機進行修改前，都要先行測試。定期進行備份以防發生任何問題。

下面這些資訊可幫助你適當調整系統核心以強化系統：

[Solaris Tunable Parameters Reference Manual \(Solaris 8\)](#)
[Solaris Tunable Parameters Reference Manual \(Solaris 9\)](#)
[Solaris Operating Environment Network Settings for Security](#)
[Solaris Kernel Tuning for Security](#) 或 <http://www.securityfocus.com/infocus/1385>

[Linux 系統核心強化\(SecurityFocus\)](#)
[Linux 系統核心倉庫](#)
[Linux 系統核心強化\(SANS\)](#)

[AIX 系統核心調整](#)

[HP-UX 系統核心調整及效能手冊](#)

<http://docs.hp.com/hpux/pdf/5185-6559.pdf>
<http://docs.hp.com/hpux/pdf/TKP-90203.pdf>
<http://docs.hp.com/cgi-bin/otsearch/hpsearch>
<http://docs.hp.com/>

[FreeBSD 手冊（包含調整系統核心的資訊）：](#)
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/index.html

[OpenBSD:](#)
<http://www.openbsd.org/faq/index.html>
<http://www.openbsd.org/docum.html> (進一步資訊)

[調整 NetBSD、調整系統核心](#)

[回頁首 ^](#)

附錄 A 常見的弱點埠號(Port)

在本節中，我們列出了最常被探測與攻擊的連接埠號(Port)。阻擋這些連接埠的網路活動僅僅只是邊境防禦(perimeter security)的最小需求，而不是完整的防火牆規則列表。更好的作法是阻擋所有未使用的連接埠，例如先拒絕所有的網路活動，再允許特定網路協定通過你的網路邊境(像是公司所需要使用到的服務)。即使你相信這些埠號已經被阻擋，你仍然應該持續進行主動監控，以察覺是否有入侵意圖。有一點要提醒你：阻擋下列清單中的連接埠可能會關閉你所需要的服務，請在進行設定前仔細考慮可能造成的潛在影響。

注意：另有一點重要且值得一提的是，一般咸認使用預設防火牆阻擋或拒絕規則，亦即未明確指定所允許的服務，會比自行設定只阻擋特定連接埠還有效得多。這同時也讓路由器與防火牆的設定與控制規則更為簡短有條理，使管理者更容易維護。

要記得阻擋這些連接埠並不是長治久安的安全政策與設計。即使連接埠被擋了，只要你的組織沒有對每一台主機都進行妥善的安全保護，攻擊者仍可以藉由其他手法獲得權限存取你的網路(像是數據機撥接、夾帶木馬的郵件、來自已過濾節點上的使用者、被操縱的內部主機等)。

名稱	埠號	協定	說明
Small services	<20	tcp/udp	小型服務
FTP	21	tcp	檔案傳輸
SSH	22	tcp	登入服務
TELNET	23	tcp	登入服務
SMTP	25	tcp	郵件
TIME	37	tcp/udp	時間同步
WINS	42	tcp/udp	WINS 複製
DNS	53	udp	名稱服務
DNS zone transfers	53	tcp	名稱服務
DHCP server	67	tcp/udp	主機設定
DHCP client	68	tcp/udp	主機設定
TFTP	69	udp	雜用
GOPHER	70	tcp	舊的類 WWW 服務
FINGER	79	tcp	雜用
HTTP	80	tcp	網頁
alternate HTTP port	81	tcp	網頁
alternate HTTP port	88	tcp	網頁(有時是 Kerberos)
LINUXCONF	98	tcp	主機設定
POP2	109	tcp	郵件
POP3	110	tcp	郵件
PORTMAP/RPCBIND	111	tcp/udp	RPC portmapper
NNTP	119	tcp	網路新聞服務
NTP	123	udp	時間同步
NetBIOS	135	tcp/udp	DCE-RPC endpoint mapper
NetBIOS	137	udp	NetBIOS name 服務
NetBIOS	138	udp	NetBIOS datagram 服務
NetBIOS/SAMBA	139	tcp	檔案共享與登入服務
IMAP	143	tcp	郵件
SNMP	161	tcp/udp	雜用
SNMP	162	tcp/udp	雜用
XDMCP	177	udp	X 圖形介面管理工具
BGP	179	tcp	雜用
FW1-secureremote	256	tcp	CheckPoint FireWall-1 mgmt
FW1-secureremote	264	tcp	CheckPoint FireWall-1 mgmt
LDAP	389	tcp/udp	名稱服務
HTTPS	443	tcp	網頁

Windows 2000 NetBIOS	445	tcp/udp	SMB 利用 IP (Microsoft-DS)
ISAKMP	500	udp	IPSEC Internet Key Exchange
REXEC	512	tcp	} 這三個是
RLOGIN	513	tcp	} 柏克萊的 r 服務程式群
RSHELL	514	tcp	} (用於遠端登入)
RWHO	513	udp	雜用
SYSLOG	514	udp	雜用
LPD	515	tcp	遠端列印
TALK	517	udp	雜用
RIP	520	udp	路由遞送協定
UUCP	540	tcp/udp	檔案傳輸
HTTP RPC-EPMAP	593	tcp	HTTP DCE-RPC endpoint mapper
IPP	631	tcp	遠端列印
LDAP over SSL	636	tcp	LDAP 利用 SSL
Sun Mgmt Console	898	tcp	遠端遙控管理
SAMBA-SWAT	901	tcp	遠端遙控管理
Windows RPC programs	1025	tcp/udp	} 這些埠號通常被
Windows RPC programs	to		} Windows 主機上的
Windows RPC programs	1039	tcp/udp	} DCE-RPC portmapper 所使用
SOCKS	1080	tcp	雜用
LotusNotes	1352	tcp	資料庫/群組軟體
MS-SQL-S	1433	tcp	資料庫
MS-SQL-M	1434	udp	資料庫
CITRIX	1494	tcp	遠端圖形介面遙控管理
WINS replication	1512	tcp/udp	WINS 複製
ORACLE	1521	tcp	資料庫
NFS	2049	tcp/udp	NFS 檔案共享
COMPAQDIAG	2301	tcp	Compaq 遠端遙控管理
COMPAQDIAG	2381	tcp	Compaq 遠端遙控管理
CVS	2401	tcp	協同檔案共享
SQUID	3128	tcp	網頁快取
Global catalog LDAP	3268	tcp	Global catalog LDAP
Global catalog LDAP SSL	3269	tcp	Global catalog LDAP SSL
MYSQL	3306	tcp	資料庫
Microsoft Term. Svc.	3389	tcp	遠端圖形介面遙控管理
LOCKD	4045	tcp/udp	NFS 檔案共享
Sun Mgmt Console	5987	tcp	遠端遙控管理
PCANYWHERE	5631	tcp	遠端遙控管理
PCANYWHERE	5632	tcp/udp	遠端遙控管理
VNC	5800	tcp	遠端遙控管理

VNC	5900	tcp	遠端遙控管理
X11	6000-6255	tcp	X Windows 伺服器
FONT-SERVICE	7100	tcp	X Windows 字型服務
alternate HTTP port	8000	tcp	網頁
alternate HTTP port	8001	tcp	網頁
alternate HTTP port	8002	tcp	網頁
alternate HTTP port	8080	tcp	網頁
alternate HTTP port	8081	tcp	網頁
alternate HTTP port	8888	tcp	網頁
Unix RPC programs	32770	tcp/udp	} 這些埠號常被 } Solaris 主機的
Unix RPC programs	到		
Unix RPC programs	32899	tcp/udp	} RPC portmapper 所使用
COMPAQDIAG	49400	tcp	Compaq 遠端遙控管理
COMPAQDIAG	49401	tcp	Compaq 遠端遙控管理
COMPAQDIAG	49401	tcp	Compaq 遠端遙控管理
PCANYWHERE	65301	tcp	遠端遙控管理

ICMP: 阻擋向內的 echo 要求(ping 和 Windows 的 traceroute), 阻擋向外的 echo 正常回應、逾時、及「目標無法到達」型態中除了「封包過長」(ICMP 型態 3 代碼 4)以外的訊息。(這樣作的原因是假設你已決定放棄使用 ICMP echo 要求訊息, 以阻擋某些惡意行為時。)

除了這些埠號外, 還需阻擋偽造的網路位址: 例如那些由外而來的封包, 其來源卻是內部位址、私有位址(RFC1918)或 IANA 保留位址(詳情請參閱 <http://www.iana.org/assignments/ipv4-address-space>)。我們也建議阻擋含有廣播位址或是多點傳送位址的封包。阻擋來源路由封包或有設 IP 標籤的封包也是個好方法。

你也應該在邊境路由器上過濾對外封包, 以阻擋由內部網路發出的偽造封包。只能允許由公司所屬指定位址發出的封包通過。

商標聲明: SANS 協會瞭解智慧財產權、商標、版權、服務商標及專利權的重要性, 並努力讓本文符合相關規範。下列的產品、系統或應用程式均以商標名稱標明。如果你覺得我們忽略了哪些具有商標的產品, 請將你的意見與發現寄到 top20@sans.org, 我們將儘快更新這份文件。

Microsoft, Windows, Windows Server 2003, Microsoft SQL Server, Microsoft Outlook 為微軟(Microsoft Corporation) 於美國與/或其他國家所屬的商標或註冊商標。

Sendmail 為 Sendmail, Inc.於美國與/或其他國家所屬的商標或註冊商標。

SSH 為 SSH Communication Security 於美國與/或其他國家所屬的商標或註冊商標。

CERT Coordination Center 為 Carnegie Mellon 軟體工程協會於美國與/或其他國家所屬的商標或註冊商標。

UNIX 為 The Open Group 於美國與/或其他國家所屬的商標或註冊商標。

[回頁首 ^](#)

附錄 B

感謝以下協助我們製作這份 2004 年清單的專家

Erik Kamerling, Project Coordinator 2003
Richard Starnes, Cable & Wireless
Ed Fisher, Ocwen Financial Corporation
Carl Thorp, Westthor
Ted Humphreys, XiSEC UK
Brian Smith-Sweeney, Smith-Sweeney Network & Security Consulting
Nick Edwards, Windsor Lodge Associates
Olivier Devaux, Qualys
Gerhard Eschelbeck, Qualys
Michael Murray, nCircle Proactive Network Security
Alexander Kotkov, Corporate Legal Services
Anton Chuvakin, Ph.D., netForensics
Kevin Hong - Korea Information Security Agency (KISA), KrCERT/CC
Dean Farrington, Wells Fargo
Cory Scott, @stake
Sam Patel, AFENTIS UK
Leo Pastor, Advanced Consulting & Training, Argentina
William Bellamy, Office of the Auditor of Public Accounts, Commonwealth of Kentucky
John Banghart, Center for Internet Security
Koon Yaw Tan, Infocomm Development Authority of Singapore
Pedro Paulo Ferreira Bueno, Brasil Telecom
Steven Sim Kok Leong, Infocomm Security Group (National University of Singapore)
Rick Wanner, SaskTel
Sanjay V. Pandit, DIRECTV
Buanzo' Busleiman, OISSG.Ar President
Scott Lawler, General Dynamics
Christopher Misra, University of Massachusetts
Jeff Ito, Department of Transportation
Rohan Amin, Lockheed Martin
Scott Fendley, Internet Storm Center
Tyler Hudak
Rohit Dhamankar, TippingPoint Technologies
Justin Tibbs, SNOsoft
Marcos A. Ferreira Jr., NX Security
Jean-Francois Legault, Connexim
Monty Ijzerman, Ph.D., McAfee, Inc.
Paul Lindsay, Philips Semiconductors
Marco Cremonini, University of Milan
Arturo Busleiman, President, OISSG Argentina

Department of Homeland Security (DHS)
British Computer Society (BCS)
Information Systems Security Association (ISSA)
Security Experts Panel (SEP)
Information Systems Security Group (ISSG)
National Infrastructure Security Coordination Centre (NISCC)
Communication Electronic Security Group (CESG)
Government Communications Headquarters (GCHQ)
Public Safety and Emergency Preparedness Canada (PSEPC)
Ministry of Defence (MoD)
Department of Defence (DoD)
Department of Transport (DoT)
Department of Energy (DoE)

Security Experts Panel (SEP)
Open Group
Security Team, ROSECURE
Information Risk Management & Audit (IRMA)

繁體中文版譯者

楊伯瀚 CISSP, Taiwan
開放式課程計畫翻譯小組 – Chinese Opensource Translation Team.(<http://www.theocw.net>)
Jess Garcia, LAEFF-INTA

中英譯名對照

英文	中文
Adware	廣告軟體
Audit Trail	稽核軌跡
Berkeley	柏克萊
Bruteforce attack	暴力猜測破解法
Buffer overflow	緩衝區溢位
Cache Poisoning	快取汙染
Cisco	思科
Cross-Site-Scripting , XSS	跨站腳本程式碼攻擊
Denial of service, DoS	阻絕服務
Dictionary attack	字典攻擊法
Directory traversal	目錄跳脫攻擊
Domain Name System, DNS	域名系統
Firewall	防火牆
Hashing algorithms	雜湊演算法
Heap	堆積
Hive (of registry)	登錄群
ISAPI extensions	ISAPI 擴充程式
Instant Messaging, IM	即時通訊
Internet	網際網路
Intrusion Detection System, IDS	入侵偵測系統
Kernal	系統核心
LAN	區域網路
Microsoft	微軟
Network Scanner	網路掃描軟體
Null session	空連線
Open Relay	開放轉發
OpenSource	開放原始碼
Operating System, OS	作業系統
Packet	封包
Peer to Peer	點對點
Perimeter security	邊境防禦
Port	連接埠
Port number	埠號
Protocol	協定
Registry	登錄值

Remote Procedure Call, RPC	遠端程序呼叫
SNMP Community String	SNMP 社群字串
SQL injection	SQL 注入攻擊
Service Pack	服務套件
Spam	垃圾郵件
Spyware	間諜軟體
Stack	堆疊
Third-party	第三方
Vulnerability	弱點
WAN	廣域網路
Web Beacons	網頁信標
Windows Domain controller	Windows 網域控制站

[回頁首 ^](#)