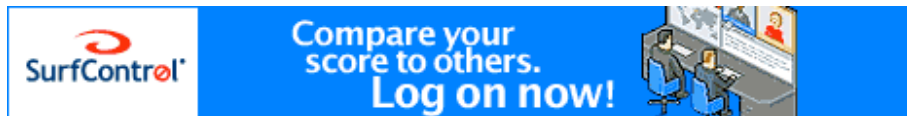


## The Top 20 Most Critical Internet Security Vulnerabilities - (2004-2005 Archive)

- [Top Vulnerabilities to Windows Systems](#)
  - [Top Vulnerabilities to UNIX Systems](#)
- [Top 20 2005 Quarter 1 Update](#)
  - [Top 20 2005 Quarter 2 Update](#)



### Introduction

The SANS Top 20 Internet Security Vulnerabilities

The vast majority of worms and other successful cyber attacks are made possible by vulnerabilities in a small number of common operating system services. Attackers are opportunistic. They take the easiest and most convenient route and exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for any vulnerable systems. The easy and destructive spread of worms, such as Blaster, Slammer, and Code Red, can be traced directly to exploitation of unpatched vulnerabilities.

Four years ago, the SANS Institute and the National Infrastructure Protection Center (NIPC) at the FBI released a document summarizing the Ten Most Critical Internet Security Vulnerabilities. Thousands of organizations used that list, and the expanded Top-20 lists that followed one, two, and three years later, to prioritize their efforts so they could close the most dangerous holes first. The vulnerable services that led to worms like Blaster, Slammer, and Code Red, as well as NIMDA worms - are on that list.

This SANS Top-20 2004 is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited elements in UNIX and Linux environments. Although there are thousands of security incidents each year affecting these operating systems, the overwhelming majority of successful attacks target one or more of these twenty vulnerable services.

The Top-20 is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts. They come from the most security-conscious government agencies in the UK, US, and Singapore; the leading security software vendors and consulting firms; the top university-based security programs; many other user organizations; and the SANS Institute. A list of participants may be found at the end of this document.

The SANS Top-20 is a living document. It includes step-by-step instructions and pointers to additional information useful for correcting the security flaws. We will update the list and the instructions as more critical threats and more current or convenient methods of protection are identified, and we welcome your input

Version 5.0 October 8, 2004

Copyright © 2005, SANS Institute

Questions / comments may be directed to [top20@sans.org](mailto:top20@sans.org).

To link to the Top 20 List, use the "SANS Top 20 List" logo

[PDF](#) | [Printer Friendly Version](#)

### Tools That Find the Top 20

Xentinel Digital Security is a leader in remote security assessment and vulnerability scanning software development, offering its HACKER FREE. Certification to companies worldwide. A large number of institutions benefit from Xentinel to help detect, analyze, resolve, and monitor vulnerabilities and compliance demands. More information at [Xentinel Digital Security](#)

### Related Resources

[Press Release - Quarter 2 Update](#)

[Top 20 2005 Quarter 2 Update](#)

[Press Release - Quarter 1 Update](#)

[Top 20 2005 Quarter 1 Update](#)

[Press Release \(PDF\)](#)

[Tools that Test for the Top 20](#)  
(Updated July 18, 2005)

[SANS Critical Internet Threats 2005](#)

[NASA Case Study](#)

### Top 20 Archive

[November, 2006 - Version 7 \(Current\)](#)

[November, 2005 - Version 6](#)

[October, 2004 - Version 5](#)

[October, 2003 - Version 4](#)

[October, 2002 - Version 3](#)

[May, 2001 - Version 2](#)

[June, 2000 - Version 1 \(Original Top 10\)](#)

### Top 20 List v5 Update Log

Oct. 18, 04 General revisions & CVE/CAN updates

Oct. 15, 04 PSEPC & CESG Statements of Support

along the way. This is a community consensus document -- your experience in fighting attackers and in eliminating the vulnerabilities can help others who come after you. Please send suggestions via e-mail to [top20@sans.org](mailto:top20@sans.org)

#### Top 20 Translations

Contact [top20@sans.org](mailto:top20@sans.org) to collaborate in the translation of the Top 20 to your own language.

[Chinese](#) - v. 5.0 - Added May 16, 2005

[Croatian](#) - v. 5.0 - Added Oct. 8, 2004

[Bulgarian](#) - v. 5.0 - Added Oct. 8, 2004

[Dutch](#) - v. 5.0 - Added Oct. 8, 2004

[German](#) - v. 5.0 - Added Oct. 8, 2004

[Italian](#) - v. 5.0 - Added Oct. 8, 2004

[Japanese](#) - v. 5.0 - Added Oct. 8, 2004

[Lithuanian](#) - v. 5.0 - Added Oct. 20, 2004

[Polish](#) - v. 5.0 - Added Oct. 8, 2004

[Portuguese](#) - v. 5.0 - Added Oct. 18, 2004

[Romanian](#) - v. 5.0 - Added Oct. 8, 2004

**NOTE:** These translations are a volunteer effort. Our deep gratitude to the individuals and organizations that invested their time and work to help the community.

## Top Vulnerabilities in Windows Systems

- [W1 Web Servers & Services](#)
- [W2 Workstation Service](#)
- [W3 Windows Remote Access Services](#)
- [W4 Microsoft SQL Server \(MSSQL\)](#)
- [W5 Windows Authentication](#)
- [W6 Web Browsers](#)
- [W7 File-Sharing Applications](#)
- [W8 LSAS Exposures](#)
- [W9 Mail Client](#)
- [W10 Instant Messaging](#)

### W1. Web Servers & Services

#### W1.1 Description

Default installations of various HTTP servers and additional components for serving HTTP requests as well as streaming media to the internet from Windows platforms have proven vulnerable to a number of serious attacks over time. The impact of these vulnerabilities can include:

- Denial of service
- Exposure or compromise of sensitive files or data
- Execution of arbitrary commands on the server
- Complete compromise of the server

HTTP servers including IIS, Apache, and iPlanet (now SunOne) have had numerous issues that have been patched as they have been discovered. Ensure that all patches are up to date for the server and that a current version is running. In most HTTP server software the default configuration is rather open leaving large avenues for exploit. Whilst this has been changed to a 'secure by default' posture for IIS 6.0, it is crucial that administrators take the time to fully understand their web server and adjust the configuration to allow only those features and services required.

#### Check Them Out!

- [SANS CDI East 2006 - Over 18 courses!](#)
- [Top 20 List](#)
- [SANS Reading Room](#)
- [Career Roadmap](#)
- [Storm Center](#)
- [WhatWorks™](#)
- [Newsletters](#)

"This is hands-down, the premiere training opportunity."  
- Dan Mather, JICPAC

IIS uses a programming hook known as ISAPI to associate files having certain extensions with DLLs (known as ISAPI extensions). Preprocessors such as ColdFusion and PHP use ISAPI, and IIS includes many ISAPI extensions to handle functions such as Active Server Pages (ASP), .Net web services, and web-based printer sharing. Many ISAPI extensions installed by default with version 5.0 and earlier of IIS are not required in most installations, and many of those filters are exploitable. Examples of malicious programs that use this type of propagation mechanism include the well-known Code Red and Code Red 2 worms. Enable only the ISAPI extensions that the web server will need to recognize and restrict the HTTP options that can be used with each allowed ISAPI extension. This tightening of security is best achieved via the [IIS LockDown](#) tool available freely from Microsoft.

Most web servers include sample applications or web sites that were designed to demonstrate the functionality of the web server. These applications were not designed to operate securely in a production environment. Versions of IIS before 6.0 include sample applications that can be exploited to allow remote viewing or overwriting of arbitrary files as well as remote access to other sensitive server information, such as system configuration settings and paths to binaries. Remove these applications prior to placing the server into production.

Any webserver installation that is not regularly maintained is also subject to vulnerabilities discovered since the software release date. Examples include the PCT and SSL vulnerabilities that are addressed by the Microsoft patch MS04-011, which could allow a Denial of Service condition or allow the attacker to take control of the server. Timely patching of publicly accessible web servers is critical.

Third-party web add-ons such as ColdFusion and php can introduce further vulnerabilities in a webserver installation, either through misconfiguration or through vulnerabilities inherent in the product.

## W1.2 Operating Systems Affected

Any Microsoft Windows system with a web server installed could be affected. This includes, but is not limited to:

- Microsoft IIS: Windows NT4.0 and above, including XP Professional
- Apache HTTP server: Windows NT4.0 SP3 and above are supported, though it is believed to run on Win95 and Win98
- Sun Java System/Sun One/iPlanet Web Server: Windows NT4.0 SP6 and above

*Please note:* Windows 2000 Server ships with IIS installed by default, as many administrators discovered during the infamous Nimda and Code Red outbreaks. As part of the Trustworthy Computing initiative, Windows Server 2003 does not enable the IIS server in a standard installation, and the default settings are configured for security. Furthermore, some third-party applications require functionality provided by IIS, possibly resulting in administrators unknowingly installing this software. Never assume a network to be immune to web server attacks simply because no such server was intentionally installed; regularly audit networks for the presence of any "rogue" web servers. See "How to Determine if you are at risk" below for more information.

## W1.3 Related CVE Entries

### a. IIS

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

Searchable [CVE entries for IIS 2.0](#), [CVE entries for IIS 3.0](#), [CVE entries for IIS 4.0](#), [CVE entries for IIS 5.0](#). To date no security exposures have been identified in IIS 6.0

### 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 modules: [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. Add-ons

[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. Other Services

[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 How to Determine if you are at risk

Any default or unpatched web server installations should be presumed vulnerable.

Most web server and service vendors provide a wealth of information regarding current security issues.

Examples include:

- Apache HTTP Server [Main Page & Security Report](#)
- Microsoft [TechNet Security Centre](#)
- Microsoft [Internet Information Server \(IIS\) Security Centre](#)
- Sun [Web, Portal, & Directory Servers Download Centre](#)
- Macromedia [Security Zone](#)
- Real Networks [Security Issues](#)
- PHP [Home Page](#) and [Downloads](#)

Also check any web server and associated service's patch and software revision levels, including configurations, against the vendor-supplied security information and the [CVE database](#) *on a regular basis* to assess potential vulnerability. It is important to realize that new issues are discovered regularly and it is best practice to consult to make good use of the [Windows Update](#) website, [Microsoft Security Baseline Analyzer](#) and [Automatic Updates](#) feature to properly assess and eliminate potential vulnerabilities.

Some remote and local vulnerability assessment tools exist to aid web server administrators in auditing their networks, including:

- [Nessus](#) (Open-source)
- [SARA](#) (Open-source)
- [Nikto](#) (Open-source)
- eEye [Free Utilities & Commercial Scanners](#)
- [Microsoft Baseline Security Analyzer](#) (which has many security benefits and features that are not just IIS-specific)

It is recommended that remote vulnerability assessment tools be run on a network-wide basis, rather than just against known servers, to assess potential vulnerability of "rogue" web server installations.

## W1.5 How to protect against these vulnerabilities

### For most systems

1. Apply the latest service packs and security updates or the HTTP service as well as for the Operating System and any applications loaded on this same host. Once the patches are up-to-date, consider using the automatic update feature to enable a higher level of security.
2. Install host-based anti-virus and Intrusion Detection software. Be sure to keep both current on patches and review the log files frequently.
3. Disable unused script interpreters and remove their binaries. For example; perl, perlscript, vbscript, jscript, javascript, and php.
4. Enable logging if it is an option and review the logs frequently, preferably through an automated process that summarizes the events and reports exceptions and suspicious events.
5. Use a syslog-like system to store Operating System and HTTPd logs safely on another system.
6. Remove or restrict the system tools that are commonly used by attackers to assist with both the initial compromise and expansion beyond the initial victim host. For example; tftp(.exe), ftp(.exe), cmd.exe, bash, net.exe, remote.exe, and telnet(.exe).
7. Limit the applications running on the host to the HTTP service/daemon and its supporting services.
8. Be aware of and minimize any vectors into the inner network that enter through public web server(s). For example, NetBIOS shares or trust relationships.
9. Use different account naming conventions and unique passwords on public facing systems than on internal systems. Any information leakage from a public facing system should not aid an attack on the internal systems.

#### a. IIS

Consider upgrading your IIS installation to IIS 6.0, which offers dramatically increased security. Patching a server on installation is necessary but not sufficient. As new IIS weaknesses are uncovered, patch accordingly. [Windows Update](#) and [Automatic Updates](#) are options for single-server installations. [Systems Management Server](#) (SMS) and [Software Update Services](#) (SUS) are also very good options for managed environments or administrators that have responsibilities for multiple disparate systems. [MBSA](#), the network security Hotfix checker, assists the system administrator in scanning local or remote systems for current patches. The tool works on Windows NT 4, Windows 2000, Windows XP and Windows 2003. The current version can be downloaded from Microsoft at <http://www.microsoft.com/technet/security/tools/mbsahome.msp>.

#### Use IIS Lockdown Wizard to harden the installation

Microsoft has released a simple tool to aid in securing IIS installations known as the IIS Lockdown Wizard. The current version can be downloaded from Microsoft at <http://www.microsoft.com/technet/security/tools/locktool.asp>

Running the IIS Lockdown Wizard in "custom" or "expert" mode will allow the following recommended changes to be made to an IIS installation:

- Ensure the latest version of WebDAV is employed on the server. IIS 6.0 allows administrators to select whether or not to enable WebDAV.
- Unmap all unnecessary ISAPI extensions (including .htr, .idq, .ism, and .printer in particular).
- Eliminate sample applications.
- Restrict permissions and the availability of binaries commonly found on a webserver and often used as part of an attack and compromise (e.g. cmd.exe and tftp.exe).

The SANS Reading Room contains the papers [Understanding and installing the IISlockdown tool](#) and [Securing a Windows 2000 IIS Web Server - Lessons Learned](#). The [Microsoft Security Centre](#) also contains a wealth of prescriptive guidance for protecting and managing IIS.

### Use URLScan to filter HTTP requests

Many IIS exploits, including Code Blue and the Code Red family use maliciously formed HTTP requests in directory traversal or buffer overflow attacks. The URLScan filter can be configured to reject such requests before the server attempts to process them. The current version has been integrated into the IIS Lockdown Wizard, but can be downloaded separately from Microsoft at <http://www.microsoft.com/technet/security/tools/urlscan.msp>.

### b. Apache

The issues of access control, restriction by IP and the Apache security modules, along with many other topics, are discussed on the [Apache Tutorials](#) page.

In addition, [Securing Apache: Step-by-Step](#) by Artur Maj is a very helpful paper found in the SANS Reading Room that covers in detail the tasks of securing an Apache server.

### c. iPlanet/Sun One

Edmundo Farinas addresses securing iPlanet in his paper [Security Considerations for the iPlanet Enterprise Web Server on Solaris](#) which is located in the SANS Reading Room.

In addition, Sun provides the [Sun ONE Application Server Security Goals](#) paper which details the recommended steps for securing an iPlanet/Sun One server.

### d. Add-ons

If third-party add-ons such as ColdFusion, PerlIIS, or PHP are used check the third-party vendors' web sites for patches and configuration tips as well. For obvious reasons, Microsoft does not include third-party patches in Windows Update and related update services.

For information on securing ColdFusion, see the SANS Reading Room paper [Web Application Security, with a Focus on ColdFusion](#) by Joseph Higgins

Located in the SANS Reading Room, [Securing PHP: Step-by-step](#) by Artur Maj illustrates the process of securing PHP applications.

In addition, a helpful resource is the [PHP Manual, Chapter 16. Security](#), which addresses PHP security in detail.

### e. Other services

While there are general steps listed above that can be taken to secure most web services, each usually has its own unique set of vendor supplied updates and patches, recommended configurations, and logging features.

Review the documentation including any information posted at the vendor's web site and make sure to sign-up for each vendor's notification service and newsletter. This will help to stay informed of relevant security issues and to address them quickly and effectively.

---

## W2 Workstation Service

### W2.1 Description

Windows Workstation service is responsible for processing user requests to access resources such as files and printers. The service determines if the resource resides on the local system or on a network share, and routes the user requests appropriately.

The network management functions provided by the service can be invoked via any of the following mechanisms.

- DCE/RPC calls over SMB protocol after connecting to the service using `\\pipe\wkssvc` named pipe.

- DCE/RPC calls directly over a UDP port (> 1024)
- DCE/RPC calls directly over a TCP port (> 1024)

*Note that the service binds to the first available TCP and UDP port over 1024.*

The Workstation service contains a stack-based buffer overflow that can be triggered by a specially crafted DCE/RPC call. The problem arises because parameters are passed to the logging function without any bounds checking. This overflow can be exploited by an unauthenticated remote attacker to execute arbitrary code on the vulnerable Windows machine with "SYSTEM" privileges. The attacker can obtain complete control of the compromised machine. The exploit code for leveraging the vulnerability has been posted to the Internet and was re-used in some variants of Phatbot/Gaobot worm that infected millions of systems world-wide.

## W2.2 Operating Systems Affected

Windows 2000 SP2, SP3 and SP4

Windows XP, Windows XP SP1

Windows XP 64 Bit Edition

## W2.3 CVE/CAN Entries

CAN-2003-0812, CAN-2003-0813, CAN-2003-0352

## W2.4 How to Determine if you are Vulnerable

Systems running Windows 2000 without the MS03-049 patch and Windows XP without the MS03-043 patch are vulnerable. Windows XP users that have installed Service Pack 2 are protected.

Check for the following registry-entries:

KB828035: Under HKLM\Software\Microsoft\Updates\Windows XP (Windows XP)

KB828749: Under HKLM\Software\Microsoft\Updates\Windows 2000 (Windows 2000)

If these registry entries are not found the Windows system may be vulnerable. For greater certainty and support in mitigating this risk, use a security scanner such as Microsoft Baseline Security Analyzer (MBSA) to check if the appropriate update has been installed. MBSA can be downloaded from

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

## W2.5 How to Protect Against It

- Windows XP Service Pack 2 offers many security enhancements that protect against these and other security risks. This should be a priority for Windows XP installations and is recommended by the [US-CERT](#).
- Ensure that Windows systems have all the latest security patches and service packs are installed. The configuration of [Automatic Updates](#) should be viewed as a necessity, tailored to fit individual or corporate requirements. Specifically ensure that Windows 2000 systems have MS03-049 and Windows XP systems have MS03-043 patch installed. As per the previous point, Service Pack 2 should be considered vital.
- Block the ports 139/tcp and 445/tcp at the network perimeter. This prevents a remote attacker from exploiting the overflow via SMB.
- Open only the necessary TCP ports over 1024 at the network perimeter. This prevents a remote attacker from exploiting the overflow via DCE/RPC calls. Note that it is difficult to block UDP ports above 1024 at the firewall as the ports in this range are used as ephemeral ports.
- Use TCP/IP Filtering available in both Windows 2000 and XP, or Windows Firewall in Windows XP systems to block inbound access to the affected ports. The Windows Firewall also offers network administrators the ability to centrally enforce policies and settings across end-user systems that can help heighten security.
- For Third-party applications running on customized Windows 2000/XP platforms ensure that an

appropriate patch from the vendor has been applied. For example, Cisco has released an advisory stating that a number of Cisco products are vulnerable to this overflow. Cisco has also provided the patches.

- g. If the system is stand-alone (i.e. does not belong to a Windows network environment), the Workstation service can be disabled, however, this must be done with caution as it can affect applications and system functionality.

#### Additional information:

Microsoft Advisory

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

eEye Advisory

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

CERT Advisories

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

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

CORE Security Advisory

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

Cisco Advisory

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

Gaobot Worm

<http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html>

---

## W3 Windows Remote Access Services

### W3.1 Description

The family of Windows Operating systems supports a variety of different networking methods and technologies. There is native support for most industry standard networking protocols and built-in functionality for many Microsoft specific networking methods and techniques. Common avenues for exploitation include Network Shares, Anonymous Logon, remote registry access, and remote procedure calls.

**NETBIOS** - A set of API's that can allow the sharing files or folders across a network with other hosts through Windows network shares. The underlying mechanism of this feature is the Server Message Block (SMB) protocol, or the Common Internet File System (CIFS). These protocols permit a host to manipulate remote files just as if they were local.

Although this is a powerful and useful feature of Windows, improper configuration of network shares may expose critical system files or may provide a mechanism for a nefarious user or program to take full control of the host. One of the ways in which I-Worm.Klez.a-h ([Klez Family](#)) worm, Sircam virus ([see CERT Advisory 2001-22](#)) and Nimda worm ([see CERT Advisory 2001-26](#)) spread so rapidly in 2001 was by discovering unprotected network shares and placing copies of themselves in them. Many computer owners unknowingly open their systems to hackers when they try to improve convenience for co-workers and outside researchers by making their drives readable and writeable by network users. But when care is taken to ensure proper configuration of network shares, the risks of compromise can be adequately mitigated.

**Anonymous Logon** - An anonymous session is a communication link established without correct credentials (i.e. blank username and password). Null sessions can be used to display information about users, groups, shares and password policies. Microsoft Windows NT services running as the Local System account on the local computer communicate with other services over the network by establishing null sessions. Windows 2000 and later services running as the Local System account on the local computer use the local computer account to authenticate to other servers.

**Remote Registry Access** - Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows 2003, Windows ME and Windows XP employ a central hierarchical database, known as the Registry, to manage software, device configurations, and user settings. Improper permissions or security settings can permit remote registry access or execution of code or applications that should not be allowed to run.

**Remote Procedure Calls** - All versions of Microsoft operating systems (Windows NT 4.0, 2000, XP, and 2003) provide an inter-process communication mechanism that allows programs running on one host to execute code on remote hosts. Three vulnerabilities have been published that would allow an attacker to run arbitrary code on susceptible hosts with Local System privileges. One of these vulnerabilities was exploited by Blaster/MSblast/LovSAN and Nachi/Welchia worms. There are also other vulnerabilities that would allow attackers to mount Denial of Service attacks against RPC components.

### W3.2 Operating Systems Affected

Windows 95, Windows 98, Windows NT Workstation and Server, Windows Me, Windows 2000 Workstation and Server, Windows XP Home and Professional, and Windows 2003 are all potentially vulnerable.

Windows XP Service Pack 2 **changed the behaviour of RPC**. A new RPC Interface Restriction was implemented to make it more secure by default. Particularly noteworthy are the addition of a new registry key - RestrictRemoteClients. This key modifies the behaviour of all RPC interfaces on the system and will, by default, eliminate remote anonymous access to RPC interfaces on the system, effectively removing this risk.

### W3.3 CVE/CAN Entries

#### NETBIOS

[CVE-2000-0979](#) (Windows 95, 98, and Windows Me - ONLY), [CAN-2003-0661](#)

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

#### Anonymous Logon

[CVE-2000-1200](#)

#### Remote Registry Access

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

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

#### Remote Procedure Calls

[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 How to Determine if you are Vulnerable

#### How to determine if you are vulnerable to NETBIOS related issues.

A number of tools are available that can help to determine if there are NETBIOS related vulnerabilities on a system.

NbtScan - NetBIOS Name Network explores the NETBIOS file-sharing services available on target systems  
NbtScan is available at: <http://www.inetcat.org/software/nbtscan.html>.

NLtest - extremely powerful tool, included in [Windows 2000 and 2003 Support Tools](#) (can be found on product CD) and [Windows NT4 Resource Kit](#). NLtest can obtain a wealth of information about potential

configuration vulnerabilities.

For Windows NT (SP4), Windows 2000, Windows XP, and Windows 2003, the [Microsoft Baseline Security Analyser](#) will report hosts that are vulnerable to SMB exploits and may be used to fix the problem. The tests can be run locally or on remote hosts.

Windows NT, Windows 2000, Windows XP, and Windows 2003 users can simply type `net share` from the command prompt to see what resources are being shared. For more information about the net share command, type `net share /?`.

**IMPORTANT Note:** This article contains information about modifying shared resources. Before modifying any shared resource, make that it is understood how to restore the resource if a problem occurs. It is recommended that any modifications are thoroughly tested before implementation in a production environment. For information about shared resources, click the following article numbers to view the article in the Microsoft Knowledge Base:

[125996 - Saving and Restoring Existing Windows Shares](#)

[308419 - HOW TO Set, View, Change, or Remove Special Permissions for Files and Folders in Windows XP](#)

[307874 - HOW TO Disable Simplified Sharing and Password-Protect a Shared Folder in Windows XP](#)

[174273 - How to Copy Files and Maintain NTFS and Share Permissions](#)

Although File System permissions and settings will take priority, the default permissions on new shares are detailed below:

Windows NT, Windows 2000, and Windows XP (Pre Service Pack 1)

- Everyone - Full Control

Windows XP SP1

- Everyone - Read

Windows XP by default has one shared directory called "SharedDocs." The physical location of this share is:

C:\Documents and Settings\All Users\WINDOWS

- The owner of the file or folder and local Computer Administrators have read and write permission to the file or folder. Nobody else may read or write to the folder or the files in it. This is the default setting for all the folders and files in each user's My Documents folder.

Most commercially-available network-based scanners will detect open shares. A quick and effective test for SMB exposures can be found at the [Gibson Research Corporation web site](#), although the accuracy of the results is dependant upon the host system not being located behind a firewall or screening device.

Automated Scanning tools to detect share vulnerabilities:

- [Nessus](#)--a free, powerful, up-to-date and easy to use remote security scanner
- [Winfingerprint by vacuum](#) --Win32 Host/Network Enumeration Scanner
- [Microsoft Baseline Security Analyser](#) - free network security tools

**How to determine if you are vulnerable to Anonymous Logon related issues.**

Try to establish a null session to the computer by issuing the following command from the command prompt (Start --> Run --> type cmd):

```
C:\>net use \\ipaddress\ipc$ "" /user:""
```

The preceding syntax connects to the hidden interprocess communications "share (IPC\$) at ipaddress

(/user:"") with a null () password.

If "The command completed successfully" is received, then the system is potentially vulnerable to remote interrogation and account enumeration.

The list of tools above, including Nessus and Winfingerprint, can also be used to detect null session vulnerabilities.

#### How to determine if you are vulnerable to Remote Registry Access related issues.

NT Resource Kit (NTRK) formerly available from Microsoft contains an executable file entitled Regdump.exe that will passively test remote registry access permissions from a Windows NT host against other Windows NT/Windows 2000 or Windows XP hosts on the Internet or internal network.

#### How to determine if you are vulnerable to Remote Procedure Call related issues.

Microsoft has made a hotfix, configuration, and patch-checking tool freely available for download; this is probably the best way to determine if Windows hosts are susceptible to any of these vulnerabilities. It is called the Microsoft Baseline Security Analyzer (MBSA) and is available from

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

There is also a standalone scanning tool that will check for missing security patches for CAN-2003-0352, CAN-2003-0528, CAN-2003-0605 and CAN-2003-0715 only; it is available from <http://support.microsoft.com/?kbid=827363>. However, it is encouraged to use the MBSA, which has a wider coverage. Home or small-scale users with only a few computers to take care of will probably find it easier to visit the Windows Update site at <http://windowsupdate.microsoft.com/> and check individual machines for outdated software.

### W3.5 How to Protect Against It

Microsoft addresses security vulnerabilities in Service Packs and security hotfixes for Operating systems and applications. It is extremely important to have the most current Service Pack installed on a system. For example, the Sasser worm and its clones (exploiting vulnerability of LSASS system) infected a lot of unpatched systems worldwide, while systems that had hotfix MS04-011 installed were immune to this extremely dangerous vulnerability. Microsoft had hotfix MS04-011 released a few weeks prior to appearance of the Sasser worm.

**NOTE:** Windows 95 and Windows NT4 Workstation are no longer supported by Microsoft. Support for Windows NT4 Server expires on December 31, 2004.

For details of lifecycle for supported operating systems and products see Microsoft article [Product Lifecycle Dates - Windows Product Family](#).

For finding relevant security hotfixes for a system, use:

- [Windows Update](#) service. It automatically detects all required security hotfixes on the system and installs them after the user selects (approves) the hotfixes that need to be installed
- Enable the [Automatic Updates](#) feature to provide enhancements to the operating system and applications as they are released by Microsoft.
- Windows Security Bulletin Search online service located at: <http://www.microsoft.com/technet/security/current.aspx>

While having current service packs and security hotfixes addresses many software design-related problems (such as buffer overflows, code design errors etc), there are a number of dangerous features in Windows OS that have legitimate and documented functionality, but can be safely disabled or secured in many cases in order to harden system security. To better understand and highlight potential security exposures or risks, employ the [Microsoft Baseline Security Analyzer \(MBSA\)](#).

#### How to protect against NETBIOS related attacks.

Several actions can be taken to mitigate the risk of exploitation of vulnerability through Windows Networking. NOTE: Extra care must be taken before disabling sharing or netbios facilities as these can have adverse effects on enterprise applications and services. In all circumstances, ensure that the changes are effectively tested before being implemented into a production environment.

If the system does not need to provide file/print services and does not need to be remotely administered (most home workstations fit into this category), the Server service can be disabled.

On Windows NT4/2000/2003/XP systems disable service Server by selecting Start - Programs - Administrative Tools - Services - select service Server - double-click it - set Startup type to value Disabled - press button Apply - press button Stop - press button OK.

If the system does require service Server running, it is recommended that systems are configured in line with current Best Practice outlined at the [Microsoft Security Guidance Center](#). In addition, the following steps can be made to secure Windows NT4/2000/2003/XP systems:

1. Enumerate all default hidden shares ( C\$, D\$, E\$ etc) by typing command:

Net share

From system command prompt. Make note of existing shares.

2. Delete default hidden shares. Note that removing hidden shares will often break enterprise applications such as backup and management applications. To ensure the shares remain deleted following a reboot, the adjustments to the registry (outlined in following steps) must be also undertaken. To delete the hidden shares, issue the following command:

Net share C\$ /delete

from system command prompt. In most cases all alphabet shares (C\$, D\$, E\$ etc) and share ADMIN\$ can be safely deleted. It is not recommended to delete default share IPC\$ on any system.

3. In order to make deletion of default shares permanent (they would be restored automatically on system restart or restart of service Server), it is necessary to make following Registry modifications:

- Open Registry editor;
- Navigate to Registry key:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
- Create new Registry value under this key:
  - Value name: AutoShareWks
  - Value type: DWord
  - Value: 00000000
- Create new Registry value under this key:
  - Value name: AutoShareServer
  - Value type: DWord
  - Value: 00000000

Review existing non-default (custom-created) shares on system. That can be done through:

- Graphical interface (My Computer - right-click - Manage - Shared Folders - Shares). Select shares that need to be disabled - right-click - select Stop Sharing.
- Command line (from system prompt or as part of any script):
  - Enumerate all shares by typing command:

Net share

From system command prompt. Make note of existing shares.

- Delete unnecessary shares by typing command:

Net share ShareName /delete

from system command prompt.

That will permanently delete non-default (custom-created) shares only. For permanent deletion of default hidden shares C\$, D\$, ADMIN\$ see procedures in previous paragraph.

- Windows 95/98/Me clients that are a part of a Windows NT domain are recommended to be setup with user-level file share access controls.
- Do not permit sharing with hosts on the Internet. Ensure all Internet-facing hosts have Windows network shares disabled in the Windows network control panel. File sharing with Internet hosts should be achieved using SCP, FTP ,or HTTP.
- Do not permit unauthenticated shares. If file sharing is required, then do not permit unauthenticated access to a share. Configure the share so a password is required to connect to the share.
- Restrict shares to only the minimum folders required. Shares should be generally only one folder and possibly sub-folders of that folder.
- Restrict permissions on shared folders to the minimum required. Be especially careful to only permit write access when it is absolutely required.
- For added security, allow sharing only to specific IP addresses as DNS names can be spoofed.

**How to protect against Anonymous Logon problems on your systems. IMPORTANT Note:** This article contains information about modifying the registry. Before modifying the registry, make sure to back it up and make sure that it is understood how to restore the registry if a problem occurs. It is recommended to thoroughly test any modifications before implementation in a production environment. For information about how to back up, restore, and edit the registry, click the following article numbers to view the article in the Microsoft Knowledge Base:

[256986 - Description of the Microsoft Windows Registry](#)

[323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0](#)

[322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000](#)

[322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003](#)

Windows NT Domain controllers require null sessions to communicate. Therefore, if working in a Windows NT domain or Windows 2000/2003 Active Directory running in mixed mode, which allows Pre-Windows 2000 compatible access, it is possible to minimize the information that attackers can obtain, but not stop all leakage by setting the RestrictAnonymous registry value to 1. For example; GetAcct from Security Friday sidesteps RestrictAnonymous=1 and will enumerate the SID and UserID. The ideal solution with a native Windows 2000/2003 Active Directory is to set the RestrictAnonymous registry value to 2.

To restrict information available via null sessions, click the following article numbers to view the articles in the Microsoft Knowledge Base:

[143474 - Restricting Information Available to Anonymous Logon Users in Windows NT](#)

[246261 - How to Use the RestrictAnonymous Registry Value in Windows 2000](#)

To troubleshoot the RestrictAnonymous registry value, click the following article number to view the article in the Microsoft Knowledge Base:

[296405 - The RestrictAnonymous Registry Value May Break the Trust to a Windows 2000 Domain](#)

#### Windows NT:

1. Start Registry Editor "regedit.exe" and go to the following subkey:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
2. Set the following registry value:  
Name: RestrictAnonymous

Type: REG\_DWORD Value: 1

3. Restart your computer.

#### Windows 2000:

1. Start "Control Panel-->Administrative Tools-->Local Security Policy".
2. Open "Local Policies-->Security Options".
3. Make sure "Additional restrictions of anonymous connections" is set to "No access without explicit anonymous permissions".
4. Restart your computer.

#### Windows XP:

1. Start "Control Panel-->Administrative Tools-->Local Security Policy".
2. Open "Local Policies-->Security Options".
3. Make sure the following two policies are enabled:
  - Network Access: Do not allow anonymous enumeration of SAM accounts
  - Network Access: Do not allow anonymous enumeration of SAM accounts and shares
4. Restart your computer.

#### How to protect against Remote Registry Access on your systems.

To address this threat, access to the system registry must be restricted and the permissions set for critical registry keys reviewed. Users of Microsoft Windows NT 4.0 should also ensure that Service Pack 4 (SP4) or later has been installed before adjusting the registry.

**Important Note:** This article contains information about modifying the registry. Before modifying the registry, make sure to back it up and make sure that it is understood how to restore the registry if a problem occurs. It is recommended to thoroughly test any modifications before implementation in a production environment. For information about how to back up, restore, and edit the registry, click the following article numbers to view the article in the Microsoft Knowledge Base:

[256986 - Description of the Microsoft Windows Registry](#)

[323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0](#)

[322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000](#)

[322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003](#)

**Restrict Network Access.** To restrict network access to the registry, follow the steps listed below to create the following Registry key:

- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\ Control\ SecurePipeServers\winreg
- Description: REG\_SZ
- Value: Registry Server

Security permissions set on this key define the Users or Groups that are permitted remote Registry access. Default Windows installations define this key and set the Access Control List to provide full privileges to the system Administrator and Administrators Group (and Backup Operators in Windows 2000).

Changes to the system registry will require a reboot to take effect. To create the registry key to restrict access to the registry:

For Windows 2000 and NT:

1. Start Registry Editor "regedit.exe" and go to the following subkey:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control
2. On the "Edit" menu, click "Add Key."
3. Enter the following values: Key Name: SecurePipeServers Class: REG\_SZ
4. Go to the following subkey:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers

5. On the "Edit" menu, click "Add Key."
6. Enter the following values: Key Name: winreg Class: REG\_SZ
7. Go to the following subkey: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
8. On the "Edit" menu, click "Add Value."
9. Enter the following values: Value Name: Description Data Type: REG\_SZ String: Registry Server
10. Go to the following subkey: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
11. Select "winreg." Click "Security" and then click "Permissions." Add Users or Groups to which to grant access.
12. Exit Registry Editor and restart Microsoft Windows.
13. If at a later stage it is required to change the list of users that can access the registry, repeat steps 10-12.

For Windows XP and 2003:

1. Start Registry Editor "regedt32.exe" and go to the following subkey: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control
2. On the "Edit" menu, click "Add Key."
3. Enter the following values: Key Name: SecurePipeServers Class: REG\_SZ
4. Go to the following subkey: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
5. On the "Edit" menu, click "Add Key."
6. Enter the following values: Key Name: winreg Class: REG\_SZ
7. Go to the following subkey: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
8. On the "Edit" menu, click "Add Value."
9. Enter the following values: Value Name: Description Data Type: REG\_SZ String: Registry Server
10. Go to the following subkey: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
11. Select "winreg." Click "Edit" and then click "Permissions." Add Users or Groups to which to grant access.
12. Exit Registry Editor and restart Microsoft Windows.
13. If at a later stage it is required to change the list of users that can access the registry, repeat steps 10-12.

**Limit Authorized Remote Access.** Enforcing strict restrictions upon the registry can have adverse side effects upon dependent services, such as the Directory Replicator and the network printer Spooler service.

It is therefore possible to add a degree of granularity to the permissions by adding either the account name that the service is running under to the access list of the "winreg" key or by configuring Windows to bypass the access restriction to certain keys by listing them in the Machine or Users value under the AllowedPaths key:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths

Value: Machine

Value Type: REG\_MULTI\_SZ - Multi string

Default Data: System\CurrentControlSet\Control\ProductOptionsSystem\

CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\

Services\EventlogSoftware\Microsoft\WindowsNT\CurrentVersionSystem\CurrentControlSet\Services\Replicator

Valid Range: (A valid path to a location in the registry)

Description: Allow machines access to listed locations in the registry provided that no explicit access restrictions exist for that location.

Value: Users

Value Type: REG\_MULTI\_SZ - Multi string

Default Data: (none)

Valid Range: (A valid path to a location in the registry)

Description: Allow users access to listed locations in the registry provided that no explicit access restrictions exist for that location.

In the Microsoft Windows 2000 and Windows XP Registry:

Value: Machine

Value Type: REG\_MULTI\_SZ - Multi string

Default Data: System\CurrentControlSet\Control\ProductOptionsSystem\

CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\ control\Server

ApplicationSystem\CurrentControlSet\Services\Eventlog\ Software\Microsoft\Windows NT\CurrentVersion

Value: Users (does not exist by default)

It is common for there to be a lag between the time a vulnerability becomes public and the time a patch is made available. Or for other policy reasons, the vulnerability must be allowed. To mitigate the risk an organization can limit access through firewalls or routers. An additional measure would be to write new rules for an IDS (Intrusion Detection System) like [Snort](#) which would alert or trigger a response by the organization. Examples of documented rules for Snort are located [here](#).

### How to protect against Remote Procedure Call-related issues on your systems.

The best way by far is to apply the relevant patches as identified by the MBSA, [Automatic Update](#) features or [Windows Update](#): see "How to determine if you are vulnerable to Remote Procedure Call related issues" above. Failing that there are a number of ways to disable or restrict some Remote Procedure Call functionality, and some can be found in the excellent synopsis at <http://www.ntbugtraq.com/dcomrpc.asp>.

BE WARNED: disabling or restricting Remote Procedure Call functionality may break Windows services that are relied on, so always test any modifications in a non-production environment first.

If systems cannot be patched, then certainly block ports associated with Windows remote procedure calls (TCP ports 135, 139, 445 and 593; UDP ports 135, 137, 138 and 445) at the network perimeters. Of course, it is always best practice to block \*all\* unnecessary services at the network perimeter by default.

For more information:

[Microsoft Knowledge Base Article 153183. How to Restrict Access to NT Registry from a Remote Computer.](#)

Another source is [Microsoft Security Bulletin Search](#).

[MSDN Library](#) (Search for Securing Registry)

[Microsoft Knowledge Base Article 310426 : HOW TO: Use the Windows XP and Windows Server 2003 Registry Editor](#)

[Network access: Remotely accessible registry paths and subpaths](#)

[Windows Server 2003 Security Guide](#)

---

## W4 Microsoft SQL Server (MSSQL)

### W4.1 Description

The Microsoft SQL Server (MSSQL) contains several serious vulnerabilities that allow remote attackers to obtain sensitive information, alter database content, compromise SQL servers, and, in some configurations, compromise server hosts.

MSSQL vulnerabilities are well-publicized and actively under attack. Two recent MSSQL worms in May 2002 and January 2003 exploited several known MSSQL flaws. Hosts compromised by these worms generate a damaging level of network traffic when they scan for other vulnerable hosts. Additional information on these worms can be found at

#### SQLSnake/Spida Worm (May 2002)

- <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](http://www.cert.org/incident_notes/IN-2002-04.html)

#### SQL-Slammer/SQL-Hell/Sapphire Worm (January 2003)

- <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>

Port 1433 and 1434 (MSSQL server and monitor default ports) have also been regularly registered as two of the most frequently scanned ports by the [Internet Storm Centre](#).

SQLSnake's exploit routine depends on the default administrative account, or "sa" account, having a null password. It is essential to the proper configuration and defence of any system to ensure that all system accounts are password protected, or completely disabled if not in use. You can find more information regarding setting and managing sa account passwords in the Microsoft Developer Network documentation under [Changing the SQL Server Administrator Login](#), as well as [Verify and Change the System Administrator Password by Using MSDE](#). The sa account should have a complex, hard-to-guess password even if it is not used to run your SQL/MSDE implementation.

SQL Slammer's exploit routine is based upon a buffer overflow in the SQL Server Resolution Service. This buffer overflow is brought to bear and host security is thus compromised when the worm sends crafted attack packets to UDP port 1434 of vulnerable target systems. If a machine runs SQL services that are subject to this stack buffer overflow and it receives packets of this nature, it will usually result in total server and system security compromise. The most effective means of defence against this worm is diligent patching, proactive system configuration practices, and ingress/egress UDP port 1434 filtering at network gateways.

The Microsoft Server 2000 Desktop Engine (MSDE 2000) can be thought of as "SQL Server Lite". Many system owners don't even realize that their systems are running MSDE and that they have a version of SQL Server installed. MSDE 2000 is installed as a part of the following Microsoft products:

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

In addition there are many other software packages that make use of the MSDE 2000 software. For an up-to-date list please check <http://www.SQLsecurity.com/applicationslistgridall.aspx>. Since this software uses MSDE as its core database engine, it has the same vulnerabilities as SQL/MSDE Server. MSDE 2000 can be configured to listen for incoming client connections in a multitude of different ways. It can be configured such that clients can use named pipes over a NetBIOS session (TCP port 139/445) or sockets with clients connecting to TCP port 1433, or both. Whichever method is used, SQL Server and MSDE will always listen on UDP port 1434. This port is designated as a monitor port. Clients will send a message to this port to dynamically discover how the client should connect to the server.

The MSDE 2000 engine returns information about itself whenever presented with the single byte packet 0x02 on UDP port 1434. Other single byte packets cause a buffer overflow without ever having to authenticate to the server itself. What further exacerbates these issues is that the attack is channelled over UDP. Whether the MSDE 2000 process runs in the security context of a domain user or the local SYSTEM account, successful exploitation of these security holes may mean a total compromise of the target system.

Since SQL Slammer exploits a buffer overflow on the target system, following best practices of timely patching and conscientious system configuration helps to mitigate this threat. By downloading and using defensive tools such as the [Microsoft SQL Critical Update Kit](#), one can check local systems for vulnerability to this exploit, scan entire domains or networks for the existence of vulnerable systems, and automatically update affected files with SQL Critical Update.

Please see the report and analysis on [incidents.org](#) for more details on the SQL/MSDE Slammer worm. This particular attack affected the Internet Backbone for a few hours on the morning of January 25, 2003.

## W4.2 Operating Systems Affected

Any Microsoft Windows system with Microsoft SQL/MSDE Server 7.0, Microsoft SQL/MSDE Server 2000 or Microsoft SQL/MSDE Server Desktop Engine 2000 installed, as well as any system which uses the MSDE engine separately.

## W4.3 CVE/CAN Entries

[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 How to Determine if you are Vulnerable

Microsoft has published a set of security tools at <http://www.microsoft.com/sql/downloads/securitytools.asp>. The toolkit named the SQL Critical Update Kit contains valuable tools such as SQL Scan, SQL Check, and SQL Critical Update.

Chip Andrews of [sqlsecurity.com](#) released a tool called SQLPingv2.2. This tool sends a single byte UDP packet (byte value of 0x02) to port 1434 of either a single host or an entire subnet. SQL Servers listening on UDP 1434 will respond by divulging system details such as version number, instances, etc. SQLPingv2.2 is considered a scanning and discovery tool much like Microsoft's SQL Scan, and will not further compromise your system and network security. Additional SQL security tools can be found at Chip Andrew's [SQL/MSDE Security Web site](#).

## W4.5 How to Protect Against It

Summary:

1. Disable SQL/MSDE Monitor Service on UDP Port 1434 (appreciate that this might interfere with remote administration or backup services).
2. Apply the latest service pack for Microsoft SQL/MSDE server and/or MSDE 2000.
3. Apply the latest cumulative patch that is released after the latest service pack.
4. Apply any individual patches that are released after the latest cumulative patch.
5. Enable SQL Server Authentication Logging.
6. Secure the server at system and network level.
7. Minimize privileges of the MSSQL/MSDEServer service and SQL/MSDE Server Agent.
8. Take Best Practice guidance on securing this infrastructure at [Microsoft](#).

## Detail:

1. Disable the SQL/MSDE Server Monitor on UDP Port 1434.

This can be easily accomplished by installing and using the functionality within [SQL Server 2000 Service Pack 3a](#). Microsoft's database engine MSDE 2000 exhibits two buffer overflow vulnerabilities that can be exploited by a remote attacker without ever having to authenticate to the server. What further exacerbates these issues is that the attack is channeled over UDP. Whether the MSDE 2000 process runs in the security context of a domain user or the local SYSTEM account, successful exploitation of these security holes may mean a total compromise of the target system. MS-SQL/MSDE Slammer sends a 376 byte long UDP packet to port 1434 using random targets at a very high rate. Compromised systems will immediately start sending identical 376 byte packets once they are infected. The worm sends traffic to random IP addresses, including multicast IP addresses, causing a Denial of Service on the target network. Single infected machines have reported traffic in excess of 50 Mb/sec after being infected.

2. Apply the latest service pack for Microsoft SQL/MSDE server and MSDE 2000.

The current Microsoft SQL/MSDE Server service pack version is:

- [SQL/MSDE Server 7.0 Service Pack 4](#)
- [MSDE/SQL Server 2000 Service Pack 3a](#)

To ensure that you are current with any future upgrades, monitor [Make Your SQL/MSDE Servers Less Vulnerable](#) from Microsoft TechNet.

3. Apply the latest cumulative patch that is released after the latest service pack.

The current cumulative patch for all versions of SQL/MSDE/MSDE Server is available at [MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks \(Q316333/Q327068\)](#).

To ensure that you are current with any future upgrades, you can check for the latest cumulative patch for Microsoft SQL/MSDE Server at:

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

Apply any individual patches that are released after the latest cumulative patch and enable the [Automatic Update](#) feature and consider subscribing the [Microsoft Security Notification Service](#). Currently, there is no individual patch after the release of the [MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks \(Q316333/Q327068\)](#).

4. Enable SQL Server Authentication Logging.

SQL Server Authentication Logging is commonly not enabled. This can be done through Enterprise Manager (Server properties; tab Security).

5. Secure the server at system and network level.

One of the most commonly attacked MSSQL/MSDE exposures is that the default administrative account (known as "sa") is installed with a blank password. If your SQL/MSDE "sa" account is not password-protected, you effectively have no security and can be affected by worms and other exploits. Therefore, you should follow the recommendation from the "System Administrator (SA) Login" topic in [SQL/MSDE Server Books Online](#) to make sure that the built-in "sa" account has a strong password, even if your SQL/MSDE server does not run using this account. Microsoft Developer's Network has documentation on [Changing the SQL Server Administrator Login](#) and how to [Verify and Change the System Administrator Password by Using MSDE](#).

6. Minimize privileges of the MSSQL/MSDEServer service and SQL/MSDE Server Agent.

Run the MSSQL/MSDEServer service and SQL/MSDE Server Agent under a valid domain account with minimal privileges, not as a domain administrator or the SYSTEM (on NT) or LocalSystem (on 2000 or XP) account. A compromised service running with local or domain privileges would give an attacker complete control of your machine and/or your network.

- a. Enable Windows NT Authentication, enable auditing for successful and failed logins, and then stop and restart the MSSQL/MSDEServer service. If possible, configure your clients to use NT Authentication.
- b. Packet filtering should be performed at network borders to prohibit specifically non-authorized inbound or outbound connections to MSSQL specific services. Ingress and egress filtering of TCP/UDP ports 1433 and 1434 could prevent internal or external attackers from scanning and or infecting vulnerable Microsoft SQL/MSDE servers on your network or the networks of others that are not explicitly authorized to provide public SQL/MSDE services.
- c. If TCP/UDP ports 1433 and 1434 need to be available on your Internet gateways, enable and customize egress/ingress filtering to prevent misuse of this port.

Additional information on securing Microsoft SQL/MSDE Server can be found at

- [Microsoft SQL/MSDE Server 7.0 Security](#)
- [Microsoft SQL/MSDE Server 2000 Security](#)

---

## W5 Windows Authentication

### W5.1 Description

Passwords, pass-phrases and security codes are used in virtually every interaction between users and information systems. Most forms of user authentication, as well as file and data protection, rely on user-supplied passwords. Since properly authenticated access is often not logged, or even if logged not likely to arouse suspicion, a compromised password is an opportunity to explore a system from the inside virtually undetected. An attacker would have complete access to any resources available to that user, and would be significantly closer to being able to access other accounts, nearby machines, and perhaps even administrative privileges. Despite this threat, accounts with bad or empty passwords remain extremely common, and organizations with good password policy are far too rare.

The most common password vulnerabilities are:

- User accounts have weak or nonexistent passwords.
- Regardless of the strength of their password, users fail to protect it.
- The operating system or third-party applications create accounts with weak or nonexistent passwords.
- In many commercial and Open Source applications, the hashing algorithms is known and often the hashes are stored where they can be accessed by standard users. Whilst system policies cannot help protect against hashing implementations or short-comings, the use of strong passwords can help thwart attacks against the hashes to recover the pass-phrase.

Microsoft Windows does not store or transmit passwords in clear text - it uses a hash of password for authentication. A Hash is a fixed-size result obtained by applying a mathematical function (the hashing algorithm) to an arbitrary amount of data (also known as the message digest). There are three Windows authentication algorithms: LM (least secure, most compatible); NTLM and NTLMv2 (most secure and least compatible). Although most current Windows environments have no need for LAN Manager (LM) support, Microsoft Windows locally stores legacy LM password hashes (also known as LANMAN hashes) by default on Windows NT, 2000 and XP systems (but not in Windows 2003). Since LM uses a much weaker encryption scheme than more current Microsoft approaches (NTLM and NTLMv2), LM passwords can be broken in a relatively short period of time by a determined attacker. Even passwords that otherwise would be considered "strong" can be cracked by brute-force in under a week on current hardware.

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/h\\_gly.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/h_gly.asp)

The weakness of LM hashes derives from the following:

- Passwords are truncated to 14 characters.

- Passwords are padded with spaces to become 14 characters.
- Passwords are converted to all upper case characters.
- Passwords are split into two seven character pieces.

This hashing implementation means that an attacker needs only to complete the trivial task of cracking two seven-character, upper-case passwords to gain authenticated access to your system. Since the complexity of cracking hashes increases geometrically with the length of the hash, each seven-character string is at least an order of magnitude simpler to attack by brute-force than would a combined fourteen-character string. Since all strings are exactly seven characters (including spaces) and entirely upper-case, a dictionary-style attack is also simplified. If the pass-phrase consists of 15 characters or more, the LM hash is sets a null string which effectively thwarts brute forcing against the hash. It is important to note that this insecurity is not just specific to Windows environments - whenever password hashes can be accessed without due authorisation, there is the potential for an attacker to brute-force the correct pass-phrase.

In addition to the risk posed by having legacy LM hashes stored in the SAM, the LAN Manager authentication process is often by default enabled on clients and accepted by servers. As a result, Windows machines capable of utilizing stronger hash algorithms instead send weak LM hashes across the network, making Windows authentication vulnerable to eavesdropping by packet sniffing, and therefore easing the efforts of an attacker to obtain and crack user passwords.

## W5.2 Operating Systems Affected

All Microsoft Windows operating systems.

## W5.3 CVE/CAN Entries

[CVE-2000-0222](#)

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

## W5.4 How to Determine if you are Vulnerable

Although there are observable symptoms of general password weakness, such as the existence of active accounts for users who have departed the organization or services which are not running, the only way to know for certain that each individual password is strong is to test all of them against the same password cracking tools used by attackers.

**Please Note:** Never run a password scanner, even on systems for which you have administrative access, without explicit and preferably written permission from your employer. Administrators with the most benevolent of intentions have been fired for running password cracking tools without authority to do so.

A few of the best cracking tools available are: [LC6 \(L0phtcrack version 5\)](#) and [John the Ripper](#)

Regarding the issue of a locally stored LAN Manager hash:

- If you are running a default installation of NT, 2000 or XP, you are vulnerable since LAN Manager hashes are stored locally, although by default only the system administrator has access privileges.
- If you have legacy operating systems in your environment that require LM authentication in order to communicate to servers, then you are vulnerable because those machines send NTLM hashes which can be sniffed off the network.

## W5.5 How to Protect Against It

The best and most appropriate defence against password weaknesses is a strong policy which includes thorough instructions to engender good password habits and proactive checking of password integrity.

- **Ensure that passwords are consistently strong.** Given enough hardware and enough time, any password can be cracked by brute force. But there are simpler and very successful ways to learn

passwords without such expense. Password crackers employ what are known as dictionary-style attacks. Since hashing methods are known, cracking utilities simply compare the hashed form of a password against the hashed forms of dictionary words (in many languages), proper names, and permutations of both. Therefore a password whose root in any way resembles a known word is highly susceptible to a password-cracking attack. Many organizations instruct users to generate passwords by including combinations of alphanumeric and special characters, and users more often than not adhere by taking a word ("password") and converting letters to numbers or special characters ("pa\$\$w0rd"). Such permutations can protect against a dictionary attack, but are likely to fall if subject to a brute-force attempt on every printable character.

A good password therefore cannot have a word or proper name as its root. A strong password policy should direct users to generate passwords from something more random, like a phrase or the title of a book or song. By concatenating a longer string (taking the first letter of each word, or substituting a special character for a word, removing all the vowels, etc.), users can generate sufficiently long strings which combine alphanumeric and special characters in a way which dictionary attacks will have great difficulty cracking. And if the string is easy to remember, then the password should be as well.

Once users are given the proper instructions for generating good passwords, procedures should be put in place to assure that these instructions are followed. The best way to do this is by validating the password whenever the user changes it by employing Passfilt (NT4).

Windows 2000, XP, 2003 have powerful tools for enforcing password policy. To view your current password policy on most Windows systems, follow these steps (Start - Programs - Administrative Tools - Local Security Policy - select Account Policies - Password Policy). The Local Security Policy has following settings:

- Password must meet complexity requirements. Determines whether passwords must meet complexity requirements. Complexity requirements are enforced when passwords are changed or created. If this policy is enabled, passwords must meet the following minimum requirements:
  - Not contain all or part of the user's account name
  - Be at least six characters in length
  - Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Nonalphanumeric characters (e.g., !, \$, #, %)
- **Enforce password history** (range: 0-24): Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords. Setting this parameter to 0 passwords remembered enables password recycling; setting it to 24 passwords remembered requires 24 changes of password before initial password can be recycled. This policy enables administrators to enhance security by ensuring that old passwords are not reused continually. To maintain the effectiveness of the password history, do not allow passwords to be changed immediately when you configure the minimum password age.
- **Maximum password age** (range: 0-999 days): Determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0.
- **Minimum password age** (range: 0-999 days): Determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 999 days, or you can allow changes immediately by setting the number of days to 0. The minimum password age must be less than the maximum password age. Configure the minimum password age to be more than 0 if you want Enforce password history to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite. The default setting does not follow this recommendation,

so that an administrator can specify a password for a user and then require the user to change the administrator-defined password when the user logs on. If the password history is set to 0, the user does not have to choose a new password. For this reason, password history is set to 1 by default.

- **Minimum password length** (range: 0-14 characters): Determines the least number of characters that a password for a user account may contain. You can set a value of between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0. Minimum password length should conform to corporate security policy (otherwise it is recommended that it be set to 8 or more characters; [National Security Agency \(NSA\)](#) recommends 12 characters).

- **Store password using reversible encryption** for all users in the domain: Determines whether Windows 2000, 2003 and XP Professional store passwords using reversible encryption. This policy provides support for applications using protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information.

An approach that can be used to automatically generate and assign complex passwords to user accounts is as follows - run the following command (from Command line prompt of Windows NT4, 2000, XP, 2003):

```
Net user username /random
```

Execution of this command will assign random complex (but always 8-characters long) passwords to an account and will print this password on the console screen. This method is usually more appropriate for assigning passwords for service accounts, rather than for actual users.

The best way to audit the quality of passwords is to run password cracking utilities in a stand-alone mode as part of routine scanning.

**Important Note:** Never run a password scanner, even on systems for which you have administrative access, without explicit and preferably written permission from your employer. Administrators with the most benevolent of intentions have been fired for running password cracking tools without authority to do so.

Once you have acquired authority to run cracking utilities on your system, do so regularly on a protected machine. Users whose passwords are cracked should be notified confidentially and given instructions on how to choose a good password. Administrators and management should develop these procedures together so that management can provide assistance when users do not respond to these notifications.

Another way to protect against nonexistent or weak passwords is to use an alternative form of authentication such as password-generating tokens or biometrics.

1. **Protect strong passwords.** Even if passwords themselves are strong, accounts can be compromised if users do not protect their passwords. Good policy should include instructions that a user never tell his or her password to anyone else, never write a password down where it could be read by others, and properly secure any files in which a password is stored to automate authentication (passwords are easier to protect when this practice is only used if absolutely necessary). Password aging should be enforced so that any passwords which slip through these rules are only vulnerable for a short window of time, and old passwords should not be reused. Make sure that the users are given warning and chances to change their password before it expires. When faced with the message "Your password has expired and must be changed," users will tend to pick a bad password.
2. **Prevent password hashes and SAM database from being copied.** Password cracking tools, mentioned in this section, obtain password hashes by:
  - Sniffing passwords from the network. Countermeasures: 1. Use of switched networks; 2. Detection and removal of network cards in promiscuous mode (they can be detected by most commercial security assessment tools, such as free tools like [ethereal](#)).
  - Copying SAM file (located in %SystemRoot%\System32\Config\ folder usually C:\Winnt\System32\Config\ - on Windows NT4 and 2000 or C:\Windows\System32\Config\ - on

Windows XP and 2003). This file is normally locked by Windows OS and can be copied only when system booted to alternative OS. SAM file also can be obtained by restoring backup of SAM file or System State (Windows 2000, 2003, XP). SAM file also located on NT4 Repair Disk.

**Countermeasures:** Limit and monitor physical access to computer systems (especially domain controllers), backup media and Repair Disk.

The following Microsoft articles provide useful references:

- [How to Disable LM Authentication on Windows NT \[Q147706\]](#) details the required changes in the registry for Windows 9x and Windows NT/2000.
- MS03-034 : Flaw in NetBIOS Could Lead to Information Disclosure (824105)
- [LMCompatibilityLevel and Its Effects \[Q175641\]](#) explains interoperability issues with this parameter.
- [How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT \[Q239869\]](#) explains how to use Windows 2000's Directory Services Client for Windows 95/98 to overcome the compatibility limitation for NTLMv2. [New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager](#)

### 3. **Tightly control accounts.**

- Any service-based or administrative accounts not in use should be disabled or removed. Any service-based or administrative accounts which are used should be given new and strong passwords.
- Audit the accounts on your systems and create a master list. Do not forget to check passwords on systems like routers and Internet-connected digital printers, copiers and printer controllers.
- Develop procedures for adding authorized accounts to the list, and for removing accounts when they are no longer in use.
- Validate the list on a regular basis to make sure no new accounts have been added and that unused accounts have been removed.
- Have rigid procedures for removing accounts when employees or contractors leave or when the accounts are no longer required.

### 4. **Maintain strong password policy for the enterprise.** In addition to operating system or network service-level controls, there are many comprehensive tools available to help manage good password policy. Many sample policies templates, policy development guidelines, password security fundamentals, and links to numerous security policy web sites (which include password policy information) can be found at the [SANS Security Policy Project](#) site.

### 5. **Disable LM authentication across the network.** The best replacement in Windows for LAN Manager authentication is NT LAN Manager version 2 (NTLMv2). NTLMv2 challenge/response methods overcome many weaknesses in LM by using stronger encryption and improved authentication and session security mechanisms. The registry key that controls this capability in both Windows NT and 2000 is:

Hive: HKEY\_LOCAL\_MACHINE  
Key: System\CurrentControlSet\Control\LSA  
Value: LMCompatibilityLevel  
Value Type: REG\_DWORD - Number  
Valid Range: 0-5  
Default: 0

Description: This parameter specifies the type of authentication to be used.

- 0 - Send LM response and NTLM response; never use NTLMv2 session security
- 1 - Use NTLMv2 session security if negotiated
- 2 - Send NTLM authentication only
- 3 - Send NTLMv2 authentication only
- 4 - DC refuses LM authentication
- 5 - DC refuses LM and NTLM authentication (accepts only NTLMv2)

On Windows 2000, 2003, and XP the same functionality can be implemented by configuring the setting LAN Manager authentication level (Windows 2000) or Network security: LAN Manager authentication level (Windows XP, 2003) (Start - Programs - Administrative Tools - Local Security Policy - Local Policies - Security Options).

If all of your systems are Windows NT SP4 or later, you can set this to 3 on all clients and 5 on all domain controllers to prevent any transmission of LM hashes on the network. However, legacy systems (such as Windows 95/98) will not use NTLMv2 with the default Microsoft Network Client. To get NTLMv2 capability, install the Directory Services Client. Once installed, the registry value name is "LMCompatibility," and the allowed values are 0 or 3.

If you cannot force your legacy clients to use NTLMv2, you can gain a slight improvement over LM hashing by forcing NTLM (NT Lan Manager, version 1) at the domain controller (set LMCompatibilityLevel to 4 or if you use tool Local Security Policy set LAN Manager authentication level to value: Send NTLMv2 Response only\Refuse LM). But the most secure option with regard to legacy systems is to migrate them to newer operating platforms, since the older operating systems do not allow this minimum security level to be supported.

6. **Prevent the LM hash from being stored.** One major problem with simply removing the LM hashes being passed over the network is that the hashes are still created and stored in the SAM or Active Directory. Microsoft has a mechanism available for turning off the creation of the LM hashes altogether, but only in Windows 2000, 2003 and XP. On Windows 2000 systems (SP2 or later), the following registry key controls this function:

Hive: HKEY\_LOCAL\_MACHINE

Key: System\CurrentControlSet\Control\LSA\NoLMHash

If this key is created on a Windows 2000 Domain Controller, the LanMan hashes will no longer be created and stored in Active Directory.

On Windows XP and 2003, the same functionality can be implemented by enabling setting Network security: Do not store LAN Manager hash value on next password change (Start - Programs - Administrative Tools - Local Security Policy - Local Policies - Security Options).

After making these modifications to a Windows 2000 system a restart is necessary for the changes to take effect.

**Important Note:** This only prevents new LM hashes from being generated. Existing LM hashes are removed individually the next time each user changes his or her password.

---

## W6 Web Browsers

### W6.1 Description

The Browser is the means by which computer users access the web on Microsoft Windows systems. The dominant web browser is Microsoft Internet Explorer (IE), which is the default web browser installed on Microsoft Windows platforms. Other Web browsers include Mozilla, Firefox, Netscape and Opera. The latest version of IE is 6, and the [US-CERT](#) has issued an advisory outlining the security enhancements and features available in IE 6. The vulnerabilities discussed here are also applicable to Mozilla versions 1.4 - 1.7.1, Firefox version 0.9.x, Netscape version 7.x, and Opera version 7.x.

The problems are six-fold:

1. Large Number of vulnerabilities over the last few years in comparison to other browsers - 153 IE vulnerabilities since April 2001, according to the [Security Focus Archive](#).
2. Longer Time to patch known IE vulnerabilities - Users have had to wait in excess of six months from

the time the vulnerability is disclosed before Microsoft issues a patch.

3. Active X and Active Scripting controls themselves have not been found to be open to particular exploitation, but can be used to bypass the security constructs of the browser and potentially impact upon the host system.
4. Large number of unpatched vulnerabilities - 34, according to <http://umbrella.name/>
5. Spyware/Adware vulnerabilities - This affects all browsers and systems that facilitate access and use of web resources.
6. Integration of IE browser into the Operating System, which makes the OS more vulnerable to exploitation.

All web browsing applications have had their share of vulnerabilities and bugs that have created security exposures. A malicious web designer can create web pages to exploit such failings while simply browsing the web pages. A prime example of this is the "Download.Ject" vulnerability, present 'in the wild' for many months, and utilized Active X vulnerabilities. Even after an exploit was published on [June 8, 2004](#), a patch for IE was not released until July, 2004. Due to its widespread use through industry and home-user environment, Microsoft Internet Explorer is by far the most attractive target for attackers. However, the majority of risks that tend to come to light, such as cross-site-scripting attacks, affect the majority of browsers in quite the same fashion. Attacks against browsers can include disclosure of cookies, local files or data, execution of local programs, download and execution of arbitrary code, or complete takeover of the vulnerable system.

## W6.2 Operating Systems Affected

These vulnerabilities exist on Microsoft Windows systems running any version of these browsers. It is important to note that IE is installed with a wide variety of Microsoft software and is therefore typically present on all Windows systems, even though the user may not wish it installed or utilized. All other browsers are installed at the user's discretion and the user decides whether the browser is used by other applications.

## W6.3 Browser Vulnerabilities, courtesy of Secunia overlap as some vulns expressed on all browsers

### A. Internet Explorer:

2004 - 15 Security Advisories (As Of July 30, 2004)

1. [Microsoft Internet Explorer Multiple Vulnerabilities](#)
2. [Internet Explorer Frame Injection Vulnerability](#)
3. [Internet Explorer File Download Error Message Denial of Service Weakness](#)
4. [Internet Explorer Security Zone Bypass and Address Bar Spoofing Vulnerability](#)
5. [Internet Explorer Local Resource Access and Cross-Zone Scripting Vulnerabilities](#)
6. [Microsoft Internet Explorer and Outlook URL Obfuscation Issue](#)
7. [Windows Explorer / Internet Explorer Long Share Name Buffer Overflow](#)
8. [Microsoft Outlook Express MHTML URL Processing Vulnerability](#)
9. [Internet Explorer/Outlook Express Restricted Zone Status Bar Spoofing](#)
10. [Multiple Browser Cookie Path Directory Traversal Vulnerability](#)
11. [Internet Explorer Cross Frame Scripting Restriction Bypass](#)
12. [Internet Explorer File Identification Variant](#)
13. [Internet Explorer Travel Log Arbitrary Script Execution Vulnerability](#)
14. [Internet Explorer File Download Extension Spoofing](#)
15. [Internet Explorer showHelp\(\) Restriction Bypass Vulnerability](#)

### B. Mozilla Vulnerabilities

2004 - 7 Secunia Advisories

1. [Mozilla Fails to Restrict Access to "shell:"](#)
2. [Mozilla XPInstall Dialog Box Security Issue](#)

3. [Multiple Browsers Frame Injection Vulnerability](#)
  4. [Mozilla Browser Address Bar Spoofing Weakness](#)
  5. [Mozilla / NSS S/MIME Implementation Vulnerability](#)
  6. [Multiple Browser Cookie Path Directory Traversal Vulnerability](#)
  7. [Mozilla Cross-Site Scripting Vulnerability](#)
- C. Netscape Vulnerabilities
- 2004 - 2 Secunia Security Advisories
1. [Mozilla Fails to Restrict Access to "shell:"](#)
  2. [Multiple Browsers Frame Injection Vulnerability](#)
- D. Opera Vulnerabilities
- 2004 - 8 Secunia Security Advisories
1. [Opera Browser Address Bar Spoofing Vulnerability](#)
  2. [Multiple Browsers Frame Injection Vulnerability](#)
  3. [Opera Address Bar Spoofing Security Issue](#)
  4. [Opera Browser Favicon Displaying Address Bar Spoofing Vulnerability](#)
  5. [Multiple Browsers Telnet URI Handler File Manipulation Vulnerability](#)
  6. [Opera Browser Address Bar Spoofing Vulnerability](#)
  7. [Multiple Browser Cookie Path Directory Traversal Vulnerability](#)
  8. [Opera Browser File Download Extension Spoofing](#)

#### W6.4 Identification and Protection from Browser Vulnerabilities

If you are using Internet Explorer on your system, there is no current way to know if you are vulnerable, due to the large number of unpatched vulnerabilities which exist. The [Windows Update Site](#) should be visited regularly and where possible the [Automatic Updates](#) feature enabled, ensuring that IE is protected from vulnerabilities that patches are available for. Users interested in further protection from browser vulnerabilities should consider employing a blend of the following recommendations:

- a. By far the most effective step towards a safe and secure browsing experience is to ensure the latest version of your web client is installed, which will feature new controls for heightened security and eliminate concerns identified in older versions of the application. For instance, the latest version of IE can be downloaded for free at: <http://www.microsoft.com/windows/ie/>
- b. Most Internet sites do not make use of ActiveX, but disabling this feature could have adverse effects on other aspects of the system. Since the [Windows Update](#) web site, which uses ActiveX, would be adversely affected by this approach, try using the "Automatic Updates" features instead. Other update options include using [Shavlik's HFNetChkPro™](#) or the [Microsoft Baseline Security Analyzer \(MBSA\)](#) to do the same. Also, online Internet Explorer analysis tools, such as the [Qualys Browser Check](#) can be very valuable in assessing the security state of IE on your systems.
- c. Comply with Best Practice recommendations and don't browse the web or access web resources when logged into the system with Administrator or high-level system privileges.
- d. If using an alternative browser is not an option, consider disabling ActiveX entirely except for internal ActiveX applets that can be preinstalled on the machine. Microsoft provides a way to stop an ActiveX control from running in Internet Explorer, and these controls are greatly enhanced for security in Windows XP SP2.

Other Browsers do not have the automated tools that are available for Internet Explorer. If one uses Mozilla/Firefox, Netscape or Opera you should check their respective web sites (<http://www.mozilla.org>, <http://www.netscape.com>, <http://www.opera.com>), or <http://umbrella.name/index.html>) for discovered vulnerabilities and fixes.

#### W6.5 How to secure Internet Explorer

To configure the Security settings for Internet Explorer start by ensuring the operating system is updated with available service packs and fixes. For XP this would involve the installation of [Service Pack 2](#):

1. Select Internet Options under the Tools menu.
2. Select the Security tab and then click Custom Level for the Internet zone.

Most of the flaws in IE are exploited through Active Scripting or ActiveX Controls.

3. Under Scripting, select Disable for "Allow paste operations via script" to prevent content from being exposed from your clipboard.

**Note:** Disabling Active Scripting may cause some web sites not to work properly.

ActiveX Controls are not as popular but are potentially more dangerous as they allow greater access to the system.

4. Select Disable for "Download signed ActiveX Controls".
5. Select Disable for "Download unsigned ActiveX Controls".
6. Also select Disable for "Initialize and script ActiveX Controls not marked as safe".

Java applets typically have more capabilities than scripts and it is good practice to ensure that system operations and maintenance are undertaken from an account that does not have Administrator privileges.

7. Under Microsoft VM, select "High safety for Java permissions" in order to properly sandbox the Java applet and prevent privileged access to your system.
8. Under Miscellaneous select "Disable for Access to data sources across domains" to help avoid simple Cross-site scripting attacks.

Please also ensure that no un-trusted sites are in the Trusted sites or Local intranet zones as these zones have weaker security settings than the other zones

---

## W7 File-Sharing Applications

### W7.1 Description

Peer to Peer File Sharing Programs (P2P) are used by a rapidly growing user base. These applications are used to download, and distribute many types of data (e.g. music, video, graphics, text, source code, and proprietary information to name a few). P2P applications have a number of legitimate uses, including the distribution of OpenSource/GPL binaries, ISO images of bootable Linux distributions, independent artists' creations, and even commercial media such as film trailers and game previews. Other times, the data is either of a questionable nature or is copyrighted. With the legal troubles experienced by Napster, the majority of these P2P programs now operate through a distributed network of clients, sharing directories of files or entire hard drives of data. Users can enter search parameters through the client software, and then one or more channels of communication are opened between participants as the client software contacts other network participants to locate the desired file. Clients participate by downloading files from other users, making their data available to others, and in some models by functioning as super-nodes which can coordinate searches for multiple users.

Peer to Peer communication consists of get requests, replies, and file transfers. A participant can concurrently perform multiple downloads while also serving multiple uploads. Searches for content can use almost any text string the user can conceive. Most of these programs currently use default ports, but can automatically or manually be set to use different ports if necessary to circumvent detection, firewalls, or egress filters. The trend seems to be moving towards the use of http wrappers to more easily bypass corporate restrictions. The multithreaded nature of searches and transfers can generate significant traffic on densely populated LANS and can completely saturate WAN links.

A number of vulnerabilities exist when using P2P software. They can be categorized into three types. Technical vulnerabilities are those that can be exploited remotely. Social vulnerabilities are those that are exploited by altering or masquerading binary content that others request. And legal vulnerabilities are those that can result from copyright infringement or objectionable material.

As mentioned above, technical vulnerabilities are those that can be exploited remotely and may result simply from a user downloading, installing, and running a programs. The CVE and CAN entries listed below all address technical vulnerabilities. These range from Denial of Service to arbitrary file access, and should be taken very seriously. Not addressed in the CVE database, but of serious concern, are the privacy and confidentiality issues that P2P applications can cause. Many of these applications include "spyware" or "adware" components that can consume even more bandwidth as they report web-surfing habits back to their makers. A poorly configured P2P client can provide unauthenticated access to your entire network by sharing mapped drives through the P2P application. There is little to no restriction on the type of data files that can be shared. Compromise of confidential information, intellectual property, and other data can result.

Social vulnerabilities exist when a malicious or previously infected user creates or alters a file to resemble something desired by another user. Virii, trojan horse programs, worms, and other malware can result. The victim of such attacks is usually the less technical user, who will "double-click" a file without noticing that the extension or icon is not what is normally associated with the data type, or that can be duped into launching an executable. Regardless of the nature of the content downloaded, users must use current anti-virus software to scan the downloads. Whenever possible, checksums should be validated to ensure that what is downloaded is what the user wanted and what the creator intended. P2P mechanisms can also used to propagate malicious code, with a number of viruses spreading by masquerading as desirable P2P content and storing themselves in the shared content folder of infected clients. P2P traffic can also tunnel command and control traffic to compromised machines (zombies.)

Legal vulnerabilities must be taken seriously by both the corporate user and the home user. Content available through P2P applications includes copyrighted music, movies, and program files. Organizations including the MPAA, RIAA, and BSA are all actively seeking to put an end to the copyright infringement occurring through P2P networks. Subpoenas for user id's, injunctions, and civil suits have all been brought in courts across the country. The success of these efforts, or lack thereof, and the morality or immorality of downloading such material must all be secondary to the costs for a company to respond to and defend against allegations of wrongdoing. Pornographic content is also widely available through the P2P networks. Whether such material is legal in your jurisdiction or not is irrelevant if a sexual harassment lawsuit is brought against your company because an employee downloaded material using a company computer that another employee found offensive.

## **W7.2 Operating Systems Affected**

There are versions of P2P software available for all Windows operating systems currently in use, along with versions for UNIX and Linux systems.

## **W7.3 CVE/CAN Entries**

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

## **W7.4 How to Determine if you are Vulnerable**

Detecting P2P activity on the network can prove to be challenging. It is possible to detect P2P software running on your network by monitoring traffic for common ports used by the software or by searching traffic for certain application layer strings commonly used by P2P software. Please see the end of this item for a listing of ports often used by P2P. There are a number of applications and services that can assist in detection or prevention of P2P traffic. Some host based intrusion prevention software can prevent the installation or execution of P2P applications. Cisco Network Based Application Recognition (NBAR) and other network based products can prevent P2P traffic from entering or leaving the network or monitor the P2P traffic. Monitoring your WAN connections with applications such as NTOP can also reveal P2P traffic. You may also wish to scan network storage locations for content commonly downloaded by users, including \*.mp3, \*.wma, \*.avi, \*.mpg, \*.mpeg, \*.jpg, \*.gif, \*.zip, \*.torrent, and \*.exe. Monitoring volumes for sudden decreases in free disk space can also be useful. Nessus also has a plug-in to detect running P2P applications, and for Microsoft Windows machines, SMS can be used to scan for executables that are installed on workstations.

## W7.5 How to Protect Against It

Corporate policy:

1. Your company should have and enforce a policy against the downloading of copyrighted material.
2. Your company should have and enforce an acceptable use policy for the corporate Internet connection.
3. Regular scanning of network storage and company workstations for unauthorized materials should be performed.

Network restrictions:

1. Regular users should not be permitted to install software, especially peer to peer applications.
2. Consider using a proxy server to control Internet access.
3. Egress filtering should restrict access to any ports not required for business purposes, although as more P2P applications move to http this will prove less effective.
4. Monitor your network for P2P traffic and address violations of policy through appropriate channels.
5. Utilize enterprise-wide antivirus software and ensure that updates are performed daily.

Common ports used by peer to peer applications

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 signature database entries at <http://www.snort.org/cgi-bin/sigs-search.cgi?sid=p2p>

ID	Title/URL
549	<a href="#">P2P napster login</a>
550	<a href="#">P2P napster new user login</a>
551	<a href="#">P2P napster download attempt</a>
552	<a href="#">P2P napster upload request</a>
556	<a href="#">P2P Outbound GNUTella client request</a>
557	<a href="#">P2P GNUTella client request</a>
559	<a href="#">P2P Inbound GNUTella client request</a>
561	<a href="#">P2P Napster Client Data</a>
562	<a href="#">P2P Napster Client Data</a>
563	<a href="#">P2P Napster Client Data</a>
565	<a href="#">P2P Napster Server Login</a>
1383	<a href="#">P2P Fastrack (kazaa/morpheus) GET request</a>
1432	<a href="#">P2P GNUTella GET</a>
1699	<a href="#">P2P Fastrack (kazaa/morpheus) traffic</a>
2180	<a href="#">P2P BitTorrent announce request</a>
565	<a href="#">P2P Napster Server Login</a>

## W8 LSAS Exposures

### W8.1 Description

The Windows Local Security Authority Subsystem Service on Windows 2000, Server 2003 and Server 2003 64 Bit, XP and XP 64 Bit editions contains a critical buffer overflow that if exploited can lead to full system compromise. This overflow is outlined in the Microsoft Security Bulletin MS04-011. This attack can be accomplished remotely and anonymously over RPC on un-patched Windows 2000 and XP systems but requires administrative privileges to be effective.

While Windows Server 2003 and Windows XP 64 bit 2003 Edition products did contain the vulnerability, the /GS overflow protection that's was added to certain parts of the OS prevented Sasser from doing any [significant damage](#) or a full system compromise.

The Local Security Authority Subsystem Service (LSASS) plays an important role in system authentication and Active Directory functionality. It is here in the interface process with Active Directory that the logging function of the LSASRV.dll can be overflowed with an inordinately long string. Potentially this vulnerability can lead to full system compromise.

The gravity of the fact that this vulnerability can be easily exploited remotely is demonstrated by the recent propagation of the LSASS based Sasser and Korgo worms. Also known as W32.Sasser (<http://www.cert.org/current/archive/2004/07/12/archive.html#sasser> , <http://www.microsoft.com/security/incident/sasser.msp>) and W32.Korgo (<http://www.cert.org/current/archive/2004/07/12/archive.html#korgo> ). Many recent malicious "bot" worms use this vulnerability for infection as well and their importance as a developing security issue is growing daily and often overlooked.

The vulnerability has been assigned CVE number CAN-2003-0533. It is strongly encouraged that network administrators not only patch their systems against this vulnerability but implement all necessary access controls at network ingress points to stop Windows RPC based abuses from entering vulnerable environments.

### W8.2 Operating Systems Affected

Windows 2000, Windows XP and Professional, Windows XP 64-Bit Edition, Windows 2003

### W8.3 CVE/CAN Entries

[CVE-1999-0227](#)

[CAN-2003-0507](#), [CAN-2003-0533](#), [CAN-2003-0663](#), [CAN-2003-0818](#)

### W8.4 How to Determine if You Are Vulnerable:

This vulnerability can either be checked across the network or locally on the system itself. A network check is best-suited to security and network administrators who need to detect vulnerable machines within a network or an IP range. A localized check suits end-users who need to detect whether their system is vulnerable.

For network based detection the following three freely-available tools can detect this vulnerability:

1. Nessus, a network-based vulnerability assessment tool, has a `smb_kb835732.nasl` plug-in (id 12209) that checks for the existence of the patch KB835732. Details and the download are available at <http://cgi.nessus.org/plugins/dump.php?id=12209>
2. DSScan from Foundstone allows a sweep of the entire network and provides a facility for alerts to be sent to vulnerable systems. Details and the download are available at

<http://www.foundstone.com/resources/proddesc/dsscan.htm>

3. Sasser Worm Scanner from eEye determines system is vulnerable to LSASS exploit and Sasser worm virus. Details and the download are available at <http://www.eeye.com/html/resources/downloads/audits/index.html>
4. The Microsoft Baseline Security Analyzer (MBSA) allows you to determine if your machine is vulnerable to this exploit. Details and the download are available at <http://www.microsoft.com/technet/security/tools/mbsahome.msp>

For localized security the use of the **Automatic Update** feature is strongly recommended, as are the following Microsoft tools.

1. The Microsoft Baseline Security Analyzer (MBSA) <http://www.microsoft.com/technet/security/tools/mbsahome.msp>
2. Windows Update scans your computer and provides you with a selection of updates tailored just for you. If MS04-011 (KB835732) is listed as one of the updates not yet installed on your machine, then your machine is vulnerable. Step-by-step instructions are available at <http://windowsupdate.microsoft.com>

## W8.5 How to Protect Against It

Summary:

1. Block ports at the Firewall
2. Apply latest patch from Microsoft
3. Enable systems advance TCP/IP filtering

Detail:

1. Block ports at the Firewall.

If you have a Firewall, you can help protect enclave networks and systems from attacks that originate from outside by blocking the following ports:

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

Perhaps the biggest hurdle involved in managing RPC security is the managing of the RPC messages themselves. RPC services run on ephemeral ports, making it almost impossible to tell a packet filter to look for RPC traffic on a specific port. One possible solution is to examine every packet to see if it contains a recognisable RPC construct, but creates a significant overhead and is relatively impractical. Another possibility is study only packets in the common RPC ephemeral port range, usually around 32,000 - 33,000. However, this has the potential to miss the traffic if the server binds to a different port.

It is suggested that you use a personal host based firewall, and then block all unsolicited inbound traffic. If you use the Internet Connection Firewall (ICF) feature in Windows XP or in Windows Server 2003 to help protect your Internet connected hosts, it blocks unsolicited inbound traffic by default. To enable the Internet Connection Firewall feature by using the Network Setup Wizard, follow these steps:

- a. Click Start, and then click Control Panel
- b. In the default Category View, click Network and Internet Connections, and then click Setup or change your home or small office network. The Internet Connection Firewall feature is enabled when you select a configuration in the Network Setup Wizard that indicates that your system is connected directly to the Internet.

To configure Internet Connection Firewall or Windows Firewall (XP SP2) manually for a connection, follow these steps:

- a. Click Start, and then click Control Panel
- b. In the default Category View, click Network and Internet Connections, and then click Network Connections.

- c. Right-click the connections on which you want to enable Internet Connection Firewall, and then click Properties
- d. Click the Advanced tab
- e. Click to select the Protect my computer or networks by limiting or preventing access to this computer from the Internet check box, and then click OK

**Note:** If you want to enable the use of some programs and services through the firewall, click Settings on the Advanced tab, and then select the programs, protocols, and services needed.

2. Apply the latest patch for LSASS depending on your Windows operating systems. The use of the [Automatic Update](#) feature is strongly recommended.

The LSASS vulnerability patch is available from the following Microsoft site.

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

3. Enabling advanced TCP/IP filtering to block all inbound traffic. To configure TCP/IP Filtering, follow these steps.
  - A. Click Start, point to Control Panel, right-click Network Connections, and then click Open.
  - B. Right-click the network connection where you want to configure inbound access control, and then click Properties
  - C. Under AdapterNameConnection Properties on the General tab, click Internet Protocol (TCP/IP), and then click Properties.
  - D. In the Internet Protocol (TCP/IP) Properties dialog box, click Advanced.
  - E. Click the Options tab.
  - F. Click TCP/IP Filtering, and then click Properties.
  - G. Click to select the Enable TCP/IP Filtering (All adapters) check box.
  - H. Under TCP/IP Filtering, there are three columns with the following labels:
    - TCP Ports
    - UDP Ports
    - IP Protocols

In each column, you must select one of the following options:

- A. Permit All. Select this option if you want to permit all packets for TCP or UDP traffic.
- B. Permit Only. Select this option if you want to permit only selected TCP or UDP traffic. Click Add, and then type the appropriate port or protocol number in the Add Filter dialog box. You cannot block UDP or TCP traffic by selecting Permit Only in the IP Protocols column and by then adding IP protocols 6 and 17.

**Note:** When you configure TCP/IP filtering, please remember which ports you need to block. For LSASS vulnerability, you must block inbound TCP/445 port.

---

## W9 Mail Client

### W9.1 Description

Microsoft Outlook is a personal information manager and email client program for Microsoft Windows. It is primarily an e-mail application, though it also provides calendar, task and contact management. When used in conjunction with a Microsoft Exchange Server, Microsoft Outlook can provide additional groupware functionality, such as supporting multiple users, helping to co-ordinate meeting times, and providing shared calendars and mailboxes.

Outlook Express (OE) is a basic email & contact management client, bundled with Internet Explorer since the earliest versions - which itself has been an integral part of all versions of Microsoft Windows starting with Windows 95. The most current version of Outlook Express, 6.0 with SP1 applied, is available as a free download from [Microsoft](#). By integrating products such as Internet Explorer and Outlook Express into other product lines, including Office, BackOffice, and the Windows operating system, Microsoft has allowed for common technologies and code to be used across the platform. Unfortunately, this practice also introduces single points of failure and heightens the impact that any single security vulnerability may pose.

One of Microsoft's goals has been to develop a usable and intuitive email and information management solution. Unfortunately, the embedded automation features are at odds with the built-in security controls (often disregarded by end-users). This has given rise to e-mail viruses, worms, malicious code to compromise the local system, and many other forms of attack.

Potential security threats of email clients include:

- Infection of computer with virus or worm - malicious code which spreads through attachments or embedded scripting in a message body;
- Spam - unsolicited commercial e-mail;
- Web beaconing - validation of email addresses triggered by opening of message by recipient.

Current versions of Outlook and Outlook Express can successfully protect users from abovementioned threats, if appropriately configured.

## W9.2 Operating Systems Affected

All versions of Microsoft Windows come with Outlook Express bundled with Internet Explorer, and are therefore potentially vulnerable.

To identify the current version of OE, start Internet Explorer and then select About Internet Explorer from the Help menu. Versions below 6 should be upgraded and updated with all appropriate security hotfixes immediately.

Outlook is only installed on a machine if the user has specifically installed it, either as a standalone application, or as part of the Microsoft Office suite. Versions of Outlook for Microsoft Windows include:

- Outlook 95
- Outlook 97
- Outlook 98
- Outlook 2000, also known as Outlook 9
- Outlook XP, also known as Outlook 10 or Outlook 2002
- Outlook 2003, also known as Outlook 11

Versions prior to Outlook 2000 are no longer supported by Microsoft Corp. and it is highly recommended to upgrade them as soon as possible to supported versions of product (Outlook 2003, 2002 or 2000).

All versions of Outlook should have latest product service pack applied.

Current version of Outlook service packs:

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

To identify the current version of Outlook, start the program and then select About Outlook from the Help menu.

Reference:

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

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

Product Lifecycle Dates [http://support.microsoft.com/default.aspx?id=fh;\[ln\];lifeprodo](http://support.microsoft.com/default.aspx?id=fh;[ln];lifeprodo)

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

[CVE-2001-1088](#), [CVE-2002-0152](#) (Macintosh - ONLY), [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-](#)

### W9.3 How to Determine if you are Vulnerable

All computers that have Internet Explorer installed will contain Outlook Express. Manual installations of Microsoft Office suite applications may include Outlook with the more common productivity packages such as Word, Excel, PowerPoint and Access.

A system may be vulnerable if either

- a. it is not fully up-to-date, which can be tested by visiting [MS update](#), or
- b. the security settings are inappropriately set

### W9.4 How to Protect Against It

There are a number of things you can do to configure Outlook and/or Outlook Express to minimize security risk.

#### Secure Outlook / Outlook Express

Each release of Outlook and Outlook Express has featured new controls for effectively safeguarding user systems and privacy. It is therefore important to ensure that clients and software are upgraded to the latest available version and that available updates are installed:

1. Routinely visit the Microsoft Update site, <http://windowsupdate.microsoft.com>, and apply all critical patches.
2. Enable [automatic updates](#) to help maintain systems stability, integrity and security.
3. Disable the Message Preview Pane by clicking on View > Layout and un-checking the "Show preview pane" option.
4. Tighten the settings relating to the Security zone associated with incoming E-mail.  
Select Tools > Options and then click on the Security Tab. Click on the "Restricted sites zone (More secure)" radio button and then manually adjust the setting to high. Click on Apply and OK to lock in your choice.

#### Protection from attachments with potentially malicious code

Versions of Outlook 2000 (SP3), Outlook 2002 (SP1 and later) and Outlook 2003 (all versions) include effective protection against attachments, that can have potentially malicious code. By default, all attachments with extensions such as .exe, .com, .vbs etc are blocked automatically. The use of an archiving tool such as WinZip or a different method of file transfer (FTP, SCP) is the recommended method if there is legitimate need to send executable file as an attachment.

A complete list of extensions, blocked by Outlook can be found in the article found at:

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

In order to extend default list of blocked file types, it is necessary to edit the Registry as follows:

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and then click the following key in the registry:

For Outlook 2003:

HKEY\_CURRENT\_USER\Software\Microsoft\Office\11.0\Outlook\Security

For Outlook XP/2002:

HKEY\_CURRENT\_USER\Software\Microsoft\Office\10.0\Outlook\Security

For Outlook 2000:

HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Outlook\Security

3. On the Edit menu, point to New, and then click String Value.
4. Type Level1Add, and then press ENTER.
5. On the Edit menu, click Modify.
6. Type <file\_name\_extensions>, and then click OK.

Note: file\_name\_extensions is a list of the attachment file name extensions. Each attachment file name extension is separated by a semicolon. For example, type .zip; .gif if you want to block both .zip and .gif files from appearing in an e-mail message as an attachment.

Microsoft Technet article KB837388 How to configure Outlook to block additional attachment file name extensions provides detailed description of this process:

<http://support.microsoft.com/?kbid=837388>

### Protection from SPAM (unsolicited commercial e-mail)

Outlook 2003 includes effective protection against Spam. In order to configure it, open Outlook - select Actions - Junk E-mail - Junk E-mail Options.

The Options tab of this dialog box has 4 radio-buttons, that control configuration and threshold of anti-spam engine:

- No Automatic Filtering - spam is not filtered out;
- Low (default setting) - quite effective setting; moves most of the junk to Junk E-mail folder and practically has very few false positives;
- High - aggressive spam filtering. Filters nearly all junk mail (sends it to folder Junk E-Mail), but can potentially label some legitimate e-mail as spam. If this level is set, it is recommended to check on regular basis folder Junk E-mail for presence of legitimate e-mail, mistakenly identified as spam;
- Safe Lists Only - only mail from senders or domains on the Safe Senders List or Safe Recipients List will be delivered to. This is the most spam-proof setting, but it requires some time and effort to populate Safe Senders List and Safe Recipients List with all legitimate addresses and domains that can communicate with the user.

Outlook Express and older versions of Outlook do not have effective anti-spam features, but they do have customizable Blocked Senders List. To set this up for Outlook Express, go to Tools > Message Rules and select Blocked Senders List.

### Protection from malicious code, embedded in text of e-mail

E-mail messages in rich-text formats (HTML, RTF) can have malicious code embedded within text, unlike plain text e-mail, which cannot include any code. The simplest and most effective way to protect against such malicious code is to read all e-mail messages in plain text format. To configure this in Outlook 2003, go to Tools > Options, and select the Preferences Tab, then the E-mail Options button, and Check Read all standard mail in plain text and Read all digitally signed mail in plain text. Press OK twice.

### Protection from Web Beaconsing

Web Beaconsing is a method of verification that an e-mail message was opened, and that therefore the recipient is a valid target for future spam, by including small pictures (usually 1x1 pixel) into the body of HTML-formatted message. This technique is widely used by spammers and advertisers. In addition to providing confirmation that a user opened the e-mail message, Web Beaconsing allows one to obtain certain information (IP address, language, version of browser) about the user and their system. To prevent Web Beaconsing on Outlook 2003, open Outlook - Select Tools > Options, and go to the Security Tab . Go to the Change Automatic Download Settings button, and Select the checkboxes Don't download pictures or other content automatically in HTML e-mail and Warn me before downloading content when editing, forwarding,

or replying to e-mail - press OK twice. Note that default Outlook 2002 has these settings configured to help protect security and user privacy.

### User Behaviour

Since it is the human element that is often the weakest link in the security process, it is important to follow some best practice guidelines when dealing with electronic mail.

When receiving an attachment, even if it has originated from a trusted source, it is important to ensure that it is screened for viruses and other malware as detailed in the following section, entitled "Anti-Virus".

Upon receipt of an attachment, save it to a folder other than My Documents, since that is what many viruses use as a starting point. Select another folder, or even another partition, to separate incoming attachments from the rest of your files.

Don't open unexpected attachments even if they are from friends. Even DOC and XLS files can contain embedded VBA macros that can cause harm to your system. If you must open the document with another Microsoft product, such as Word, be sure to go under Tools > Options > Security and select the radio button next to High to disable macros unless they are signed. By default unsigned macros are not allowed to run on systems.

Always check all available digital signatures associated with executable files to ensure file integrity and to verify that it has originated from a trusted source.

### Anti-Virus

Antivirus software can help protect computers against most viruses, worms, Trojan horses, and other malicious code. It is crucial that antivirus signature databases be updated at least weekly (and ideally automatically and daily) to help protect against even the newest threats. Most modern antivirus solutions fully automate this task. It is prudent to ensure that all files are scanned as a precautionary measure, regardless of file-type or origin.

Modern anti-virus solutions have the ability to scan all incoming and outgoing mail to ensure that malicious file-types and scripts are blocked before they can harm the local system.

It is highly recommended that up-to-date virus protection tools are installed before using e-mail or other Internet services, as many viruses spread through e-mail clients in the form of attachments or malicious scripted code that is run when a message is read or previewed.

Reference:

Microsoft Antivirus Reference <http://www.microsoft.com/security/protect/antivirus.asp>

### Update Outlook and Outlook Express

Outlook Express has been upgraded several times over the years, providing greater built-in functionality, stability and security. The most recent version is freely available at <http://www.microsoft.com/windows/oe/> and comes bundled with XP Service Pack 2.

To ensure that Outlook and all of your other Office programs are completely up-to-date, visit the [Office Product Updates page](#). This site automatically detects critical and recommended updates as necessary.

For detailed information about other security features and settings in Office 2003, read the [Office 2003 Security white paper](#).

**Note:** One should contact one's system administrator before making changes to any managed computer. Administrators can find detailed technical information about the Outlook E-Mail Security Update in the [Office Resource Kit](#).

### Uninstall Outlook

If one uses a separate e-mail or information management client then Outlook may be safely uninstalled.

### Outlook on all versions of Windows

Outlook may be removed from by clicking on Start > Settings > Control Panel and double clicking on the

Add/Remove Programs icon. When the Add/Remove Program Properties dialog box opens, click on the Outlook tab and select the Remove button.

### Outlook Express on Windows 98/ME

Outlook Express may be removed from the system by clicking on Start > Settings > Control Panel and double clicking on the Add/Remove Programs icon. When the Add/Remove Program Properties dialog box opens, click on the Windows Setup tab and scroll down the window to Microsoft Outlook Express and remove the check mark in the box next to it.

Click on the Apply and OK buttons to lock in your changes and Windows will uninstall Outlook Express.

Outlook Express on Windows 2000/XP or Updated versions of Internet Explorer The steps necessary to remove Outlook Express under Windows 2000/XP or for users who have upgraded their browser to a later version are much more complex. Refer to the following Microsoft guides for full details:

Windows 2000 users running Microsoft Outlook Express versions 5.x/6.0

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q263837>

Windows 98/Me and updated to Microsoft Outlook Express versions 5.x/6.0

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q256219>

**Note: Outlook Express may be re-installed silently if a service pack, significant roll-up, or operating system upgrade is installed.**

---

## W10 Instant Messaging

### W10.1 Description

Instant Messaging technology has matured over the last few years from a novel add on application that enabled users to quickly stay in touch with friends and family, to a core Windows Operating System capability often used for business communication, collaboration, and operational support. While third party Instant Messaging (IM) applications still hold a large share of IM deployments, there is a growing trend to integrate Messaging functionality into the Operating System itself which can potentially pose a direct security threat to organizations that have acceptable use policies or secure operational frameworks that deny the use of this technology. The discovery of vulnerabilities in these programs also poses a significant risk to organizations that lack the technical countermeasures, security staff, or capabilities to mitigate this increasingly embedded threat.

By far, a great majority of IM applications found on Windows systems are Yahoo! Messenger (YM), AOL Instant Messenger (AIM), MSN Messenger (MSN) and Windows Messenger (WM) which is now fully integrated into Windows XP Professional and Home Editions. The capabilities that these programs bring to the desktop are wide ranging and may provide users with the ability to check remote web based email, do voice chat, perform video communication, and send and share data files above and beyond simple text based chatting. There is also a growing trend of "multi network" messaging programs that provide the user with a centralized interface to disparate messaging networks and protocols, like Trillian and the recently formed AOL, Yahoo!, and MSN chat alliance, which enabled all three clients to interact seamlessly in the workplace.

Remotely exploitable vulnerabilities in these programs or associated dependencies are a growing threat to the integrity and security of networks, directly proportional to their rapid integration and deployment on Windows systems. Attack scenarios for Instant Messaging vulnerabilities are widely varied, and can come in the form of remotely executed buffer overflows (RPC based, packet malformation), URI/malicious link based attacks, file transferring vulnerabilities, and Active X exploits.

Vulnerabilities in these programs typically arise from the following categories:

- Outdated ActiveX controls - e.g. MSN Messenger "ResDLL" Buffer Overflow CAN-2002-0155, Yahoo! Voice Chat ActiveX Control Buffer Overflow Vulnerability (<http://www.securityfocus.com/bid/7561>), Yahoo! Webcam ActiveX Control Buffer Overrun Vulnerability (<http://www.securityfocus.com/bid/8634>).

- URI implementation problems - e.g. Yahoo! Messenger malicious script execution CAN-2002-0032, Yahoo! Messenger URI handler buffer overflow CAN-2002-0031.
- Various Buffer Overflows, such as those resulting from file transfers. - e.g. MSN Messenger file validation failure CAN-2004-0122, Yahoo! Messenger "Imvironment" and "message" field buffer overflows respectively CAN-2002-0320 and CAN-2002-0320, AOL Instant Messenger TLV 0x2711 packet parsing buffer overflow CAN-2002-0005, VU#912659, Yahoo! Messenger YAuto.DLL Open Buffer Overflow Vulnerability (<http://www.securityfocus.com/bid/9145>), AOL Instant Messenger Getfile Screenname Buffer Overrun Vulnerability (<http://www.securityfocus.com/bid/8825>)

These applications not only introduce network based vulnerabilities into systems but also pose an intellectual property loss risk, potential for loss of confidentiality, and threat of employee productivity loss. While mitigating remotely exploitable weaknesses in these programs is of utmost importance, the necessary acceptable use policy and ingress/egress traffic enforcement is also of paramount importance to ensure one avoids the problems that Instant Messaging can introduce into a network.

### W10.2 Operating Systems Affected:

Windows 98, Windows ME, Windows 2000 and Professional, Windows XP and Windows 2003 are capable of running the Microsoft Instant Messenger. All versions of Microsoft Windows XP come with Instant Messenger bundled with operating system.

### W10.3 CVE/CAN Entries:

[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 How to Determine if You Are Vulnerable:

To identify the current version of Microsoft Instant Messenger, start the application and then select About Instant Messenger from the Help menu. Versions below 6.2 should be upgraded and updated with all appropriate security hotfixes immediately.

### W10.5 How to Protect Against It:

- Ensure that any installed messenger software such as Yahoo, MSN, AOL, Trillian etc is up-to-date with all vendor patches.
- Configure any Intrusion Prevention/Detection system to alert on any file transfers that use any of the messaging programs.
- If the appropriate site security policy permits, block the following ports at the firewall. Note that this does not offer a complete protection as some of these applications can bypass firewall rules.
  - 1863/tcp: Microsoft .NET Messenger, MSN Messenger
  - 5050/tcp: Yahoo Messenger
  - 6891/tcp: MSN Messenger File Transfers
  - 5190-5193/tcp: AOL Instant Messenger
- Block access to webpages containing links with URLs such as "aim:" or "ymsgr:". This can prevent exploitation of the flaws in the URI handlers. Another option is to carefully remove just these registry keys in the "HKEY\_CLASSES\_ROOT".
- Block access to webpages invoking ActiveX controls associated with any messenger problems. This can prevent exploitation of vulnerabilities in the ActiveX controls associated with messenger programs.

# Top Vulnerabilities in UNIX Systems

- U1 BIND Domain Name System
- U2 Web Server
- U3 Authentication
- U4 Version Control Systems
- U5 Mail Transport Service
- U6 Simple Network Management Protocol (SNMP)
- U7 Open Secure Sockets Layer (SSL)
- U8 Misconfiguration of Enterprise Services NIS/NFS
- U9 Databases
- U10 Kernel

---

## U1. BIND Domain Name System

### U1.1 Description

The Berkeley Internet Name Domain (BIND) package has become the worlds most widely used implementation of the Domain Name Service (DNS). DNS is a critical system that facilitates the conversion of hostnames (e.g. [www.sans.org](http://www.sans.org)) into the corresponding registered IP address.

Since many DNS servers are Internet facing, they are a popular target for the attackers. Even though these servers are critical to any organization, surveys show that an excessive number of outdated, mis-configured and/or vulnerable servers still remain in production [1]. Hence, many of the DNS servers are still vulnerable to attacks that have been published since past few years. The attacks range from denial-of-service i.e. attacks that can crash the named daemon via a malformed DNS request or response, to buffer overflows and cache poisoning. Note that the BIND development team has historically been quick to respond to and/or repair vulnerabilities.

### U1.2 Operating Systems Affected

Just about every UNIX and Linux system is distributed with some version of BIND. BIND is also available for the Windows platform.

### U1.3 CVE/CAN Entries

[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 How to Determine if you are Vulnerable

Any DNS server running a version of BIND that was bundled with the operating system, should be compared against the current patches released by the appropriate vendor. If a running version of BIND is compiled from source from [Internet Software Consortium \(ISC\)](#), it should be checked to ensure it is the latest version. Outdated and/or un-patched versions of BIND are most likely vulnerable.

On most system implementations, the command "named -v" will show the installed BIND version enumerated as X.Y.Z where X is the major version, Y is the minor version, and Z is a patch level. Currently the three major versions for BIND are 4, 8 and 9. If on is running a BIND server built from source, one should avoid using version 4, opting instead for version 9. You can retrieve the latest source, version 9.3.0, from [ISC](#).

A proactive approach to maintaining the security of BIND is to subscribe to any of the customized alerting

and vulnerability reports, such as those available from [SANS](#), Secunia or by keeping up with advisories posted at [OSVDB](#). In addition to security alerts, an updated vulnerability scanner can be highly effective in diagnosing any potential vulnerabilities in the DNS systems.

## U1.5 How to Protect Against It

- To generally protect against BIND vulnerabilities:
  - Apply all vendor patches or upgrade DNS servers to the latest version. For more information about hardening a BIND installation, see the articles about securing name services as referenced in [CERT's UNIX Security Checklist](#).
  - Apply appropriate firewall rules for any DNS servers inside a network that are not required to be accessible from the Internet.
  - To secure the zone transfers between a primary and a secondary DNS server in a cryptographic way, configure the servers to use the DNS Transaction Signatures (TSIG). The TSIG option is available only in BIND version 8.2 and later.
  - Jail: To prevent a compromised BIND service from exposing ones entire system, restrict BIND so that it runs as a non-privileged user in a chroot()ed directory. For BIND 9, see <http://www.losurs.org/docs/howto/Chroot-BIND.html>.
  - Disable recursion and glue fetching to defend against DNS cache poisoning.
- To protect against the BIND vulnerabilities discovered in the last couple of years:
  - Cache poisoning via negative responses: <http://www.kb.cert.org/vuls/id/734644>
  - For the Denial of Service Vulnerability in ISC BIND 9: <http://www.cert.org/advisories/CA-2002-15.html>
  - For the Denial of Service Vulnerability in ISC BIND 8: <http://www.isc.org/products/BIND/bind-security.html>

There exist many excellent guides to hardening BIND. One excellent guide on hardening BIND on Solaris systems, as well as additional references for BIND documentation, can be viewed at [Running the BIND9 DNS Server Securely](#) and the archives of BIND security papers available from [AFENTIS](#). You can also view documentation covering general BIND security practices including TSIG configuration at [http://www.linuxsecurity.com/resource\\_files/server\\_security/securing\\_an\\_internet\\_name\\_server.pdf](http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf).

### References:

[1] DNS Version Survey  
<http://mydns.bboy.net/survey/>

---

## U2. Web Server

### U2.1 Description

HTTP traffic is by far the most common use of the public internet. Unix web servers such as Apache and the Sun Java System Web Server (formerly iPlanet) serve a majority of that traffic, and as such deserve close scrutiny regarding security issues. These issues include vulnerabilities within the server itself, as well as add-on modules, default/example/test cgi scripts, PHP bugs, and various other attack vectors.

While many such vectors exist, the overarching and largest cause of compromise of a Unix web server is the result of a system which is misconfigured at install time or not regularly maintained. The result of such compromise can be anything from Denial of Service, to web site defacement, to complete root access to the server by the attacker, and everything in between.

Various vendors and open-source projects provide best-practice configuration and ongoing security updates to their products, and it is vital that any web site administrator be vigilant in keeping current on. It is important to realize that most web servers are compromised via well-known, public exploits which take advantage of vulnerabilities long-since patched or otherwise managed by the vendor.

## U2.2 Affected Operating Systems

All UNIX systems are capable of running an HTTP server. Many Linux and UNIX variants come with Apache installed and enabled by default. Additionally, both Apache and iPlanet/Java System are capable of running on a host of other operating systems including Windows and is likely subject to many of the same vulnerabilities.

## U2.3 CVE/CAN Entries

NOTE: As mentioned, both Apache and iPlanet/Java System are capable of running on multiple platforms. Users of these servers should consult the appropriate "CVE/CAN Entries" of this list item as well as the Windows list item W1.3 to ensure that all possible vulnerabilities are accounted for.

### 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](#)

### Other

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

## U2.4 How to Determine if you are Vulnerable

Any default or unpatched web server installations should be presumed vulnerable.

The best way to keep current on security issues for a given product is to consult that vendor's security information page. Examples of such pages include:

- Apache HTTP Server [Main Page & Security Report](#) (Includes links to [ApacheWeek](#))
- Sun Web, Portal, & Directory Servers [Download Center & BigAdmin Portal](#)
- PHP [Home Page](#) and [Downloads](#)
- [OpenSSL](#)

Any vulnerability listed should be dealt with as soon as possible. The window of time between when a vulnerability is announced and a public exploit becomes available, and further when a worm abusing that exploit is released into the world, is growing ever smaller.

To aid in the process of vulnerability assessment, one can leverage any one of several available vulnerability scanners, including [Nessus](#) and [SARA](#) (both open-source), or any of the [Free Utilities](#) or [Commercial Scanners](#) available from eYE. Such scans should be run network-wide, to enable an administrator to gauge risk from known and unknown servers.

## U2.5 How to Protect Against It

1. Ensure that all webservers are running the latest patch level; see "How to Determine if you are Vulnerable" for links to appropriate vendor's sites

2. Disable any and all unnecessary functionality in the server. Of particular interest is CGI access, php support, mod\_ssl and mod\_proxy (for Apache). Disable them all by default, only enabling them when service demands it!
  - If PHP, CGI, SSI or other scripting languages are necessary, consider utilizing suEXEC. suEXEC allows scripts to be run under Apache with a user id other than the Apache user id.
  - **WARNING:** It is imperative that suEXEC is understood thoroughly. If it is improperly utilized it can create new security holes.
3. For Apache 1.3.x see <http://httpd.apache.org/docs/suexec.html>
4. For Apache 2.0.x see <http://httpd.apache.org/docs-2.0/suexec.html>
5. Secure the content of cgi-bin and other scripts directories. All sample and default scripts should be removed.
6. Secure PHP:

This is a broad topic in and of itself. What follows gives some sound starting points for ensuring your PHP implementation is secure.

  1. Disable parameters that will cause PHP to disclose information in the HTTP header.
  2. Ensure that PHP is running in safe mode.  
Detailed information can be found here:  
<http://www.securityfocus.com/printable/infocus/1706>
7. Additional modules can aid in securing Apache. The mod\_security ([www.modsecurity.org](http://www.modsecurity.org)) module can help protect against Cross Site Scripting (XSS) and SQL injection. Detailed implementation instructions can be found at their website.
8. Auditing scripts for vulnerabilities including XSS and SQL injection is also important. There are a few open source tools that will accomplish this. Nikto (available at <http://www.cirt.net/code/nikto.shtml>) is one of the more comprehensive CGI scanning tools.
9. One should consider running HTTP servers in a chroot environment. If an HTTP server is started chroot-ed it cannot access any part of the operating system directory structure outside of the chroot. This can often help prevent exploits. For example, an exploit may call a shell and since /bin/sh likely does not (and should not) reside in the chroot, it would be ineffective.  
**WARNING:** chrooting may have adverse effects on CGI, PHP, databases and other modules or communications which may require the web server environment access to external libraries or binaries. As there are numerous methods of chrooting, software documentation should be consulted for assistance. Additional information can be found below.
  - <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](http://www.sun.com/software/whitepapers/webserver/wp_ws_security.pdf)
10. Do not run your web server as "root" or under an account with super-user privileges. A unique user and group with minimal privileges should be created for running the webserver and no other system processes should be run under this user or group (e.g. run Apache as the user apache instead of the user nobody).
11. **Limit the server information that is revealed.**

While this suggestion tends to encounter opposition from people suggesting security by obscurity is not an acceptable method of risk mitigation, and a number of exploit attempts seen on the public internet are done in a blind sweeping fashion (proven by the fact that one will see in many Apache logs IIS exploit attempt after IIS exploit attempt), there are also some exploits that will trigger based on header information.

  - To modify the default Apache HTTP response token.
    - For Apache 1.3.x see <http://httpd.apache.org/docs/mod/core.html#servertokens>  
<http://httpd.apache.org/docs/mod/core.html#serversignature>.
    - For Apache 2.0.x see <http://httpd.apache.org/docs-2.0/en/mod/core.html#servertokens>.
  - Ensure that mod\_info is not accessible from the Internet.
    - Directory indexing should be disabled.
  - Efficient and thorough logging is essential to effectively track down any potential security

problems or unexplained behavior one may be experiencing with ones web server. It is a good practice to routinely rotate logs and keep older logs archived. This will make the log size more manageable and easier to parse if necessary.

Various information regarding log formats and rotation are available here:

- For Apache 1.3.x see: <http://httpd.apache.org/docs/logs.html>
- For Apache 2.0.x see: <http://httpd.apache.org/docs-2.0/logs.html>

In many scenarios the content of these logs may not be sufficient. Especially when using PHP, CGI or other scripting it is a good idea to log GET and POST payloads. This can yield important data and evidence in the event of a security compromise. Logging of GET and POST payloads can be implemented via mod\_security (for Apache).

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

## Check Them Out!

- [SANS CDI East 2006](#)  
- Over 18 courses!
- [Top 20 List](#)
- [SANS Reading Room](#)
- [Career Roadmap](#)
- [Storm Center](#)
- [WhatWorks™](#)
- [Newsletters](#)

"This is hands-down, the premiere training opportunity."

- Dan Mather, JICPAC

Contact us: (301) 654-SANS(7267)  
Monday - Friday 9am-5pm EST/EDT