

## SANS Top-20 Internet Security Attack Targets (2006 Annual Update)

### Operating Systems

- W1. Internet Explorer
- W2. Windows Libraries
- W3. Microsoft Office
- W4. Windows Services
- W5. Windows Configuration Weaknesses
- M1. Mac OS X
- U1. UNIX Configuration Weaknesses

### Cross-Platform Applications

- C1 Web Applications
- C2. Database Software
- C3. P2P File Sharing Applications
- C4 Instant Messaging
- C5. Media Players
- C6. DNS Servers
- C7. Backup Software
- C8. Security, Enterprise, and Directory Management Servers

### Network Devices

- N1. VoIP Servers and Phones
- N2. Network and Other Devices Common Configuration Weaknesses

### Security Policy and Personnel

- H1. Excessive User Rights and Unauthorized Devices
- H2. Users (Phishing/Spear Phishing)

### Special Section

- Z1. Zero Day Attacks and Prevention Strategies



### Introduction

Six 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 relied on that list, and on the expanded Top-20 lists that followed in succeeding years, 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 have been on SANS Top20 lists.

The SANS Top-20 2006 list is not "cumulative." We have listed only critical vulnerabilities from the past year or so. If you have not patched your systems for a length of time, it is highly recommended that you patch the vulnerabilities listed in the Top-20 2005 list as well as those in the 2006 list. At the end of this document, you will find a short SANS Top-20 FAQ (frequently asked questions) that answers questions you may have about the project and the way the list is created.

The SANS Top-20 2006 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

Version 7.0 November 15, 2006

Copyright © 2006, 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](#)

#### Want to receive updates to the Top20 list?

Subscribe to the Top20 mailing list at:

<http://lists.sans.org/mailman/listinfo/top20-announce>

#### Related Resources

[SANS Top 20 FAQ](#)

[Press Release \(2006-11-15\)](#)

#### Top 20 In The News

Please check back

#### Top 20 Archive

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

[November, 2005 - Version 6](#)

[October, 2004 - Version 5](#)

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; the Internet Storm Center, and many other user organizations. A list of participants is 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 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)

[October, 2003 - Version 4](#)

[October, 2002 - Version 3](#)

[May, 2001 - Version 2](#)

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

#### **Top 20 List v7 Update Log**

2006-11-15 - v7.0: Initial Release

#### **Top 20 Translations**

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

## **W1. Internet Explorer**

### **W1.1 Description**

Microsoft Internet Explorer is the most popular browser used for web surfing and is installed by default on each Windows system. Unpatched or older versions of Internet Explorer contain multiple vulnerabilities that can lead to memory corruption, spoofing and execution of arbitrary scripts. The most critical issues are the ones that lead to remote code execution without any user interaction when a user visits a malicious webpage or reads an email. Exploit code for many of the critical Internet Explorer flaws are publicly available. In addition, Internet Explorer has been leveraged to exploit vulnerabilities in other core Windows components such as HTML Help and Graphics Rendering Engine. Vulnerabilities in ActiveX controls installed by Microsoft or other vendor software are also being exploited via Internet Explorer.

These flaws have been widely exploited to install spyware, adware and other malware on users' systems. The spoofing flaws have been leveraged to conduct phishing attacks. In many cases, the vulnerabilities were zero-days i.e. no patch was available at the time the vulnerabilities were publicly disclosed. The VML **zero-day** vulnerability fixed by Microsoft patch MS06-055 was widely exploited by malicious websites before the patch was available.

During the past year Microsoft has released multiple updates for Internet Explorer.

- Vulnerability in Vector Markup Language Could Allow Remote Code Execution ([MS06-055](#))
- Cumulative Security Update for Internet Explorer ([MS06-042](#))
- Vulnerability in Microsoft JScript Could Allow Remote Code Execution ([MS06-023](#))
- Cumulative Security Update for Internet Explorer ([MS06-021](#))
- Cumulative Security Update for Internet Explorer ([MS06-013](#))
- Cumulative Security Update for Internet Explorer ([MS06-004](#))
- Cumulative Security Update for Internet Explorer ([MS05-054](#))

Note that the latest cumulative update for Internet Explorer includes all the previous cumulative updates.

Although [MS06-051](#) is a patch for Windows kernel, it is important for Internet Explorer; without this patch, a denial-of-service vulnerability in Internet Explorer can be reliably exploited to execute arbitrary code.

### **W1.2 Operating Systems Affected**

Internet Explorer 5.x and 6.x running on Windows 98/ME/SE, Windows NT Workstation and Server, Windows 2000 Workstation and Server, Windows XP Home and Professional, and Windows 2003 are all potentially vulnerable.

### **W1.3 CVE Entries**

[CVE-2005-2831](#), [CVE-2006-0020](#), [CVE-2006-1185](#), [CVE-2006-1186](#), [CVE-2006-1188](#), [CVE-2006-1189](#), [CVE-](#)

[2006-1245](#), [CVE-2006-1303](#), [CVE-2006-1313](#), [CVE-2006-1359](#), [CVE-2006-1388](#), [CVE-2006-2218](#), [CVE-2006-2382](#), [CVE-2006-2383](#), [CVE-2006-3450](#), [CVE-2006-3451](#), [CVE-2006-3637](#), [CVE-2006-3638](#), [CVE-2006-3639](#), [CVE-2006-3873](#), [CVE-2006-4868](#)

## W1.4 How to Determine If You Are at Risk

Use any vulnerability scanner to check whether your systems are patched against these vulnerabilities. You can also consider using the Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) or Systems Management Server ([SMS](#)) to check the security patch status of your systems.

## W1.5 How to Protect against These Vulnerabilities

- If you are using Internet Explorer on your system, the best way to remain secure is to upgrade to Windows XP Service Pack 2. The improved operating system security and Windows Firewall will help mitigate risk. For those unable to use Windows XP with Service Pack 2, it is strongly recommended that another browser be used.
- It is also recommended to upgrade to version 7 of Internet Explorer, which provides improved security over previous versions. The latest version of Internet Explorer, IE7, is being distributed by Microsoft as a Critical Update ([KB926874](#))
- Keep the systems updated with all the latest patches and service packs. If possible enable [Automatic Updates](#) on all systems.
- Watching out for [Microsoft Security Advisories](#) and implementing suggested mitigations before the patch becomes available could alleviate exposure to zero day attacks.
- To prevent exploitation of remote code execution vulnerabilities at Administrator level, tools like Microsoft [DropMyRights](#) can be used to implement "least privileges" for Internet Explorer.
- Prevent vulnerable ActiveX components from running inside Internet Explorer via the "killbit" mechanism.
- Many spyware programs are installed as Browser Helper Objects. A Browser Helper Object or BHO is a small program that runs automatically every time Internet Explorer starts and extends its functionalities. Browser Helper Objects can be detected with Antispyware scanners.
- Use Intrusion Prevention/Detection Systems, Anti-virus, Anti-Spyware and Malware Detection Software to block malicious HTML script code.
- Windows 98/ME/NT are no longer supported for updates. Legacy users should consider upgrading to Windows XP.
- Consider using other browsers such as Mozilla Firefox that do not support ActiveX technology.

## W1.6 How to Secure Internet Explorer

To configure the Security settings for Internet Explorer:

- Select Internet Options under the Tools menu.
- 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.
- 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.

- Select Disable for Download signed and unsigned ActiveX Controls. Also select Disable for Initialize and script ActiveX Controls not marked as safe.
- Java applets typically have more capabilities than scripts. Under Microsoft VM, select High safety for Java permissions in order to properly sandbox the Java applet and prevent privileged access to your system.
- Under Miscellaneous select Disable for Access to data sources across domains to avoid Cross-site scripting attacks.
- 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.

## W1.7 References

### Internet Explorer Security Updates

- <http://www.microsoft.com/technet/security/Bulletin/MS06-055.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=38#widely1>
- <http://www.microsoft.com/technet/security/Bulletin/MS06-042.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=32#widely2>
- <http://www.microsoft.com/technet/security/bulletin/MS06-023.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=24#widely5>
- <http://www.microsoft.com/technet/security/bulletin/MS06-021.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=24#widely1>
- <http://www.microsoft.com/technet/security/Bulletin/MS06-013.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=12#widely1>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=11#widely4>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=12#widely1>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=15#widely1>
- <http://www.microsoft.com/technet/security/Bulletin/MS06-004.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=6#widely1>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely2>
- <http://www.microsoft.com/technet/security/Bulletin/MS05-054.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=50#widely1>

### US-CERT Securing Web Browser Information

- [http://www.us-cert.gov/reading\\_room/securing\\_browser/browser\\_security.html](http://www.us-cert.gov/reading_room/securing_browser/browser_security.html)

---

## W2. Windows Libraries

### W2.1 Description

Windows libraries are modules that contain functions and data that can be used by other modules such as Windows applications. Windows applications typically leverage a large number of these libraries often packaged as dynamic-link library (DLL) files to carry out their functions. These libraries usually have the file extension DLL or OCX (for libraries containing ActiveX controls).

DLLs provide a way to modularize applications so that their functionality can be updated and reused easily. DLLs also help to reduce memory overhead when several applications use the same functionality at the same time. These libraries are used for many common tasks such as HTML parsing, image format decoding and protocol decoding. Local as well as remotely accessible applications use these libraries. Thus, a critical

vulnerability in a library usually impacts a range of applications from Microsoft and third-party vendors that rely on that library. Often the exploitation is possible via multiple attack vectors. For instance, the flaws in image processing libraries can be exploited via Internet Explorer, Office and image viewers. In most cases, the libraries are used by all flavors of Windows operating systems, which increase the number of systems available for attacks.

During the past year, several windows libraries were reported to have critical vulnerabilities. In a number of cases, exploit codes were discovered before patches were available (**zero-day**).

In December 2005, a vulnerability (CVE-2005-4560) was reported in the Graphics Rendering Engine: when handling specially crafted Windows Metafile (WMF) images, it could cause arbitrary code to be executed. Several malicious exploits and malwares were discovered spreading widely over the Internet soon after the discovery. As this vulnerability can be exploited by simply viewing a malicious WMF image file (through websites or attachments), many applications were reported to be affected. Even some of the Lotus Notes versions were reported to be affected by this WMF zero-day exploit. A patch was not available until early January 2006. Details of this vulnerability and exploits can be found at: <http://isc.sans.org/diary.php?storyid=993>.

As vulnerabilities in Windows libraries can be exploited in multiple vectors, in many cases a remote attacker will just need to persuade a user to access a specially crafted website, image, icon, or cursor file and the attacker would be able to execute arbitrary code on that user's system, with their privileges.

The critical libraries affected during past year include:

- Vulnerability in Windows Explorer Could Allow Remote Execution ([MS06-057](#), [MS06-015](#)).
- Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution ([MS06-050](#))
- Vulnerability in HTML Help Could Allow Remote Code Execution ([MS06-046](#))
- Vulnerability in Microsoft Windows Could Allow Remote Code Execution ([MS06-043](#))
- Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution ([MS06-026](#), [MS06-001](#))
- Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution ([MS06-002](#))

## W2.2. Operating Systems Affected

Windows NT, Windows 2000, Windows XP, Windows 2003

## W2.3. CVE Entries

[CVE-2005-4560](#), [CVE-2006-0010](#), [CVE-2006-0012](#), [CVE-2006-2376](#), [CVE-2006-2766](#), [CVE-2006-3086](#), [CVE-2006-3357](#), [CVE-2006-3438](#), [CVE-2006-3730](#), [CVE-2006-4868](#)

## W2.4. How to Determine If You Are at Risk

- Use any vulnerability scanner to check whether your systems are patched against these vulnerabilities. You can also consider using the Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) or Systems Management Server ([SMS](#)) to check the security patch status of your systems.
- You can also verify the presence of a patch by checking the registry key mentioned in the Registry Key Verification section of the corresponding security advisory. Additionally, it is advisable to also make sure the updated file versions mentioned in the advisory are installed on the system.

## W2.5. How to Protect against These Vulnerabilities

- Ensure that your Windows systems have all the latest security patches installed.
- Block the ports 135-139/tcp, 445/tcp and other ports used by Windows systems at the network

perimeter. This prevents a remote attacker from exploiting the vulnerabilities via shared file systems.

- Use TCP/IP Filtering available in Windows 2000 and XP, Windows Firewall in Windows XP systems or any third party personal firewall to block inbound access to the affected ports. It is important that the firewall is properly configured to block against external attacks effectively.
- Intrusion Prevention/Detection Systems as well as anti-virus and malware detection software are very helpful in providing additional protection from malware and exploits that are exploiting these vulnerabilities.
- If you are running third-party applications on customized Windows 2000/XP platforms, ensure that an appropriate patch from the vendor has been applied.
- Follow the principle of "Least Privilege" to limit worms and Trojans from getting a foothold on any systems. Further details about limiting access to certain registry keys, executables and directories are available in the NSA guides at <http://www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1>.
- Use system hardening guidelines (such as those from [CISecurity](#) ) to make systems more resistant to remote and local attacks.
- Keep up-to-date on Microsoft security news and patches (<http://www.microsoft.com/security/default.msp> ).
- Due to the large number of attack vectors, be vigilant when receiving email attachment from unsolicited emails and surfing to unknown websites. Do not click on unsolicited links received in emails, instant messages, web forums, or internet relay chat (IRC) channels.
- Windows NT is no longer supported. Users should upgrade to Windows XP/2003.

## W2.6. References

Vulnerability in Windows Explorer Could Allow Remote Execution

<http://www.microsoft.com/technet/security/Bulletin/MS06-057.msp>

<http://www.microsoft.com/technet/security/Bulletin/MS06-015.msp>

Vulnerability in Vector Markup Language Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/Bulletin/MS06-055.msp>

Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/bulletin/MS06-050.msp>

<http://www.microsoft.com/technet/security/bulletin/MS05-015.msp>

Vulnerability in HTML Help Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/Bulletin/MS06-046.msp>

<http://www.microsoft.com/technet/security/bulletin/MS05-026.asp>

<http://www.microsoft.com/technet/security/bulletin/MS05-001.asp>

Vulnerability in Microsoft Windows Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/bulletin/MS06-043.asp>

Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/bulletin/MS06-026.asp>

<http://www.microsoft.com/technet/security/bulletin/MS06-001.asp>

<http://www.microsoft.com/technet/security/bulletin/MS05-053.asp>

Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/bulletin/MS06-002.asp>

---

## W3. Microsoft Office

### W3.1 Description

Microsoft Office is the most widely used email and productivity suite worldwide. The applications include Outlook, Word, PowerPoint, Excel, Visio, FrontPage and Access. Vulnerabilities in these products can be exploited via the following attack vectors:

- The attacker sends the malicious Office document in an email message. Viruses can exploit this attack vector.
- The attacker hosts the document on a web server or shared folder, and entices a user to browse the webpage or the shared folder. Note that Internet Explorer automatically opens Office documents. Hence, browsing the malicious webpage or folder is sufficient for the vulnerability exploitation.
- The attacker runs a news server or hijacks a RSS feed that sends malicious documents to email clients.

A large number critical flaws were reported last year in MS Office applications. Moreover, a few of them ([CVE-2006-5296](#), [CVE-2006-4694](#), [CVE-2006-4534](#), [CVE-2006-3649](#), [CVE-2006-3590](#), [CVE-2006-3059](#), [CVE-2006-2492](#), [CVE-2006-1540](#), [CVE-2006-1301](#)) were exploited at a **zero-day** stage when no fix was available from the vendor, which represents a growing trend. Exploit code and technical details are publicly available for some of these vulnerabilities.

The critical flaws that were reported last year in Office and Outlook Express are:

- PowerPoint Remote Code Execution Vulnerability ([CVE-2006-5296](#))
- Word Malformed Stack Vulnerability ([MS06-060](#))
- Office and PowerPoint Mso.dll Vulnerability ([MS06-062](#), [MS06-048](#))
- Excel Multiple Remote Code Execution Vulnerabilities ([MS06-059](#))
- PowerPoint Malformed Record Vulnerability ([MS06-058](#))
- Visio, Works and Projects VBA Vulnerability ([MS06-047](#))
- Office Malformed String Parsing Vulnerability ([MS06-038](#))
- Excel Malformed SELECTION record Vulnerability ([MS06-037](#))
- Word Malformed Object Pointer Vulnerability ([MS06-027](#))
- Outlook and Exchange TNEF Decoding Remote Code Execution ([MS06-003](#))

### W3.2 Operating Systems Affected

Windows 9x, Windows 2000, Windows XP, Windows 2003 are all vulnerable depending on the version of Office software installed.

### W3.3 CVE Entries

[CVE-2006-5296](#), [CVE-2006-4694](#), [CVE-2006-4534](#), [CVE-2006-3649](#), [CVE-2006-3590](#), [CVE-2006-3059](#), [CVE-2006-2492](#), [CVE-2006-1540](#), [CVE-2006-1301](#), [CVE-2006-0002](#)

### W3.4 How to Determine If You Are at Risk

The MS Office installations running without the patches referenced in the Microsoft Bulletins listed from the NVD entries are vulnerable. Use any vulnerability scanner to check whether your systems are patched against these vulnerabilities. You can also consider using the Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) or Systems Management Server ([SMS](#)) to check the security patch status of your systems.

### W3.5 How to Protect against the Microsoft Office Vulnerabilities

- Keep the systems updated with all the latest patches and service packs. If possible enable [Automatic Updates](#) on all systems.
- [Disable](#) Internet Explorer feature of automatically opening Office documents.
- Configure Outlook and Outlook Express with enhanced [security](#).
- Use Intrusion Prevention/Detection Systems and Anti-virus and Malware Detection Software to prevent malicious server responses and documents from reaching the end users.
- Use mail and web filtering systems at the network perimeter to prevent malicious Office documents from reaching end-user systems.

## W3.6 References

Microsoft Office zero-day Discussions

<http://blogs.technet.com/msrc/archive/2006/10/12/poc-published-for-ms-office-2003-powerpoint.aspx>

<http://blogs.securiteam.com/?p=508>

[http://www.symantec.com/enterprise/security\\_response/writeup.jsp?docid=2006-081616-2104-99](http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-081616-2104-99)

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FMDROPPER%2EBI&Vsect=T>

<http://blogs.securiteam.com/?p=451>

[http://www.symantec.com/security\\_response/writeup.jsp?docid=2006-051911-0706-99](http://www.symantec.com/security_response/writeup.jsp?docid=2006-051911-0706-99)

[http://www.symantec.com/security\\_response/writeup.jsp?docid=2006-051914-5151-99](http://www.symantec.com/security_response/writeup.jsp?docid=2006-051914-5151-99)

---

## W4. Windows Services

### W4.1 Description

The family of Windows Operating systems supports a wide variety of services, networking methods and technologies. Many of these components are implemented as Service Control Programs (SCP) under the control of Service Control Manager (SCM), which runs as Services.exe. Vulnerabilities in these services that implement these Operating System functions are one of the most common avenues for exploitation.

Several of the core system services provide remote interfaces to client components through Remote Procedure Calls (RPC). They are mostly exposed through named pipe endpoints accessible through the Common Internet File System (CIFS) protocol, well known TCP/UDP ports and in certain cases ephemeral TCP/UDP ports. Historically, there have been many vulnerabilities in services that can be exploited by anonymous users. When exploited, these vulnerabilities afford the attacker the same privileges that the service had on the host.

Earlier versions of the operating system, especially Windows NT and Windows 2000, enabled many of these services by default for a better out of the box experience. These non essential services increase the exploit surface significantly.

The critical vulnerabilities were reported in the following Windows Services within the past year:

- Server Service ([MS06-040](#), [MS06-035](#))
- iRouting and Remote Access Service ([MS06-025](#))
- Exchange Service ([MS06-019](#))

Exploit code is available for these vulnerabilities. For instance, the vulnerability addressed by hotfix [MS06-040](#) was exploited by the worms [W32.Dasher.G](#) and [W32.Spybot.AKNO](#).

### W4.2 Operating Systems Affected

Windows 2000 Workstation and Server, Windows XP Home and Professional, and Windows 2003 are all potentially vulnerable.

### W4.3 CVE Entries

[CVE-2006-0027](#), [CVE-2006-1314](#), [CVE-2006-2370](#), [CVE-2006-2371](#), [CVE-2006-3439](#)

### W4.4 How to Determine If You Are at Risk

- Use any vulnerability scanner to check whether your systems are patched against these vulnerabilities. You can also consider using the Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) or Systems Management Server ([SMS](#)) to check the security patch status of your systems.
- You can also verify the presence of a patch by checking the registry key mentioned in the Registry Key Verification section of the corresponding security advisory. Additionally, it is advisable to also make sure the updated file versions mentioned in the advisory are installed on the system.
- To check if your system is vulnerable to an issue in an optional service, you need to determine if the service is enabled. This can be done through the Service Manager interface, which can be invoked from **Services** in Administrative Tools.

### W4.5 How to Protect against the Windows Services Vulnerabilities

- Keep the systems updated with all the latest patches and service packs. If possible enable [Automatic Updates](#) on all systems.
- Use Intrusion Prevention/Detection Systems to prevent/detect attacks exploiting these vulnerabilities.
- In some cases, exposure to the vulnerability could be removed by disabling the corresponding service. For example, Windows Routing and Remote Access service could be disabled in most environments using Windows 2000. To do so, start the service manager interface. Locate the required service and right click it. Invoke the properties option in the popup menu. The "Startup Type" of the service can be modified to disable the respective service.
- In some cases, null session access to the vulnerable interface could be removed as a work-around. It is a good practice to review your current RestrictAnonymous settings and keep it as stringent as possible based on your environment. <http://www.securityfocus.com/infocus/1352>
- Many of these vulnerabilities are found on interfaces offered through CIFS, and blocking ports 139/tcp and 445/tcp at the perimeter is essential for preventing remote attacks. It is also a good practice to block inbound RPC requests from the Internet to ports above 1024 to block attacks to other RPC based vulnerabilities using [firewalls](#).
- XP SP2 and Windows 2003 SP1 and R2 come with several security enhancements, including the Windows firewall and Security Configuration Wizard (Windows 2003 SP1 and R2 only). It is highly advisable to upgrade to these service packs, enable the Windows firewall and reduce attack surface with Security Configuration Wizard.

### W4.6 References

Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP

<http://www.microsoft.com/technet/security/topics/serversecurity/tcg/tcgch00.msp>

Windows XP Security Guide

<http://www.microsoft.com/technet/security/prodtech/windowsexp/secwinxp/default.msp>

Windows Server 2003 Security Guide

<http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.msp>

Using Windows Firewall

<http://www.microsoft.com/windowsxp/using/networking/security/winfirewall.msp>

Security Configuration Wizard for Windows Server 2003

<http://www.microsoft.com/windowsserver2003/technologies/security/configwiz/default.msp>

How to use IPSec IP filter lists in Windows 2000

<http://support.microsoft.com/kb/313190>

How to block specific network protocols and ports by using IPSec

<http://support.microsoft.com/kb/813878>

How to configure TCP/IP filtering in Windows 2000

<http://support.microsoft.com/kb/309798>

---

## W5 Windows Configuration Weaknesses

### W5.1 Description

#### 1. User Configured Password Weaknesses

Weaknesses in password configurations have taken on added importance in recent years with the proliferation of worms, bots, and other malware which have improved their ability to propagate themselves through the abuse of inadequate passwords. Enforcement of complex passwords is one of the oldest issues facing IT security administrators but continues to plague enterprises across the globe. These weaknesses can exist at both the Active Directory and the local level, each of which can be exploited effectively both by malware and by inside threats. In addition, with the increase of cross-platform centralized authentication, compromise of Windows credentials can often lead directly to compromise of credentials for other platforms (i.e. UNIX and RACF/ACF2/Top Secret). Even if complex passwords are enforced on the vast majority of accounts on the network, one weak password can lead to a much larger compromise.

#### 2. Service Account Passwords

Non-system Service accounts need passwords in Windows. Unfortunately, it is still very common to use short, printable passwords for these accounts. This is particularly troublesome as they are often used on many machines, have high privileges, and change rarely.

#### 3. Null Log-on

Null credentials have long been an issue in Windows domain environments. Since the inception of the domain architecture with Windows NT, null sessions have allowed anonymous users to enumerate systems, shares, and user accounts. Windows 2000 introduced two levels of control over anonymous access; however, this control was disabled by default. With the inception of Windows 2003, Microsoft has added a number of controls over anonymous access and enabled some restrictions by default. However, legacy systems have forced many environments to continue to support anonymous connections.

### W5.2 How to Protect Against Configuration Weaknesses

#### Weak Passwords:

- Enforce a strict password policy for all users on the domain. This policy should include complexity requirements and password expiration. Consider using a 3rd party tool for managing local account passwords and ensuring that passwords are unique.
- Prevent Windows from storing the LM hash in Active Directory or SAM database by following the [instructions](#) posted by Microsoft.
- Implement a policy to periodically test passwords across the enterprise. This testing should include the use of automated tools such as [THC Hydra](#), [LophtCrack](#) and [John the Ripper](#) to check

for blank and simple/common passwords. The testing should be performed on all platforms and should not be limited to AD passwords.

## Null Log-on:

- Restrict anonymous access to domain systems. See the "References" section for details regarding the impact of null session restrictions and the settings available in various scenarios.

## W5.3 References

The Administrator Accounts Security Planning Guide

<http://www.microsoft.com/technet/security/topics/serversecurity/administratoraccounts/default.aspx>

Windows Security Guides

<http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.aspx>

[http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-](http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en)

[A0201F639A56&DisplayLang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en)

How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases

<http://support.microsoft.com/kb/299656>

MSRPC NULL sessions - exploitation and protection

[http://www.hsc.fr/ressources/presentations/null\\_sessions/null\\_sessions\\_explained.html](http://www.hsc.fr/ressources/presentations/null_sessions/null_sessions_explained.html)

Restricting Anonymous Access

[http://technet2.microsoft.com/WindowsServer/en/library/2c82586e-bd58-42b7-9976-](http://technet2.microsoft.com/WindowsServer/en/library/2c82586e-bd58-42b7-9976-228a23721e351033.aspx?mfr=true)

[228a23721e351033.aspx?mfr=true](http://technet2.microsoft.com/WindowsServer/en/library/2c82586e-bd58-42b7-9976-228a23721e351033.aspx?mfr=true)

Client, service, and program incompatibilities that may occur when you modify security settings and user rights assignments

<http://support.microsoft.com/kb/823659>

Microsoft policy on third-party security configuration guidance support

<http://support.microsoft.com/kb/885409/en-us>

---

## M1. Mac OS X

### M1.1 Description

Mac OS X is Apple's BSD-based operating system for its line of PowerPC- and Intel-based computers.

For more information on Mac OS X, see: <http://www.apple.com/macosx>

Mac OS X is made up of many different components. Each of these components could potentially have security flaws. The majority of the critical flaws discovered in the past year fall into six different categories:

- Safari - Apple's Safari web browser is the default web browser in recent versions of Mac OS X. Vulnerabilities in this application could potentially result in complete control of a user's browser or login session.
- ImageIO - The core image-handling framework used by the system and most applications. Vulnerabilities in this framework could potentially affect many different applications. Image files are generally considered "safe" files by various applications, and are opened without prompting by default.
- Unix - Mac OS X is based on and incorporates large amounts of code from earlier Unix-like operating systems. Many applications written for various Unix and Unix-like operating systems run

on Mac OS X and some of these applications are shipped as part of the operating system by Apple. Flaws in these applications may be patched for Mac OS X considerably later than for the upstream vendor.

- **Wireless** - Reports of a critical vulnerability in Mac OS X's wireless network subsystem that allow physically-proximate attackers to gain complete control of a vulnerable system were met with surprise by many in the security community. The nature of the flaw allowed attackers to attack systems even if that system was not part of the same logical network as the attacker. Additional flaws were discovered in the Bluetooth wireless interface subsystem, with similar results.
- **Virus/Trojan** - The first viruses and trojans for the Mac OS X platform were discovered in the past year.
- **Other** - The remaining vulnerabilities do not fit in a well-defined category.

Note that Apple normally distributes patches and updates as comprehensive updates; a given Security Update will include both low-severity and critical updates.

## M1.2 CVE Entries

### Safari Vulnerabilities (includes zero-days)

HTML Rendering Vulnerabilities - [CVE-2005-3705](#), [CVE-2006-1987](#), [CVE-2006-3505](#), [CVE-2006-3946](#)

Security Bypass Vulnerabilities - [CVE-2005-2516](#), [CVE-2006-0399](#), [CVE-2006-0397](#), [CVE-2006-0398](#).

### ImageIO Vulnerabilities

Image Format Vulnerabilities - [CVE-2006-1469](#), [CVE-2006-1982](#), [CVE-2005-2747](#)

### 3rdParty Products' Vulnerabilities

Inherited Vulnerabilities - [CVE-2006-0384](#)

### Wireless Driver Vulnerabilities

WiFi Driver Vulnerabilities - [CVE-2006-3509](#), [CVE-2006-3508](#), [CVE-2006-3507](#)

### Viruses and Trojans

Viruses and Trojans - [OSX/Leap-A](#) trojan.

### Other Vulnerabilities

[CVE-2006-3498](#), [CVE-2006-1450](#), [CVE-2006-1449](#), [CVE-2006-0848](#), [CVE-2005-2518](#), [CVE-2006-4394](#)

## M 1.3 How to Determine if You Are at Risk

Any default or unpatched Mac OS X installations should be presumed to be vulnerable.

The following procedure will check if there are new packages available.

1. Choose System Preferences from the Apple Menu.
2. Choose Software Update from the View menu.
3. Click Update Now.
4. Check the items available

To aid in the process of vulnerability assessment, you can leverage any vulnerability scanner.

## M1.4 How to Protect Against These Vulnerabilities

- Be sure to stay current and have all security updates for Apple products applied by turning on the Software Update System to automatically check for software updates released by Apple. Although different schedules are possible, we recommend that you configure it to check for updates on a weekly basis at least. For more information about how to check and run the Software Update System, see the Apple Software Updates webpage - <http://www.apple.com/macosex/upgrade/softwareupdates.html>
- To avoid unauthorized access to your machine, turn on the built-in personal firewall. If you have authorized services running in your machine that need external access, be sure to explicitly permit them.
- There are many excellent guides available for hardening Mac OS X. The [CIS Benchmark](#) for Mac OS X enumerates security configurations useful for hardening the Operating System. The actions suggested by the CIS Level-1 benchmarks documents are unlikely to cause any interruption of service or applications and are highly recommended to be applied on the system. Also, the [Securing Mac OS X 10.4 Tiger](#) white paper examines security features and hardening of Mac OS X.

---

## U1. UNIX Configuration Weaknesses

### U1.1 Description

Most Unix/Linux systems include a number of standard services in their default installation. These services, even if fully patched, can be the cause of unintended compromises. Security savvy administrators harden systems by turning off unnecessary services and/or firewalling them from the Internet.

For example a default installation of Red Hat Enterprise Linux will have services such as cups (Common Unix Printing System), portmap (RPC support), sendmail (Mail Transport Agent), and sshd (OpenSSH server) which should be disabled if they are not required.

Of particular interest are **brute-force attacks against command line access such as SSH, FTP, and telnet**. These services are often the target of attacks due to the prevalence of these services for remote access. However over the last couple of years a concerted effort has been made by attackers to brute-force the passwords used by these applications. Increasingly worms and bots have brute force password engines built into them. Systems with weak passwords for user accounts are actively compromised; often privilege escalations are used to gain root access, and root-kits installed to hide the compromise. It is important to remember that brute forcing passwords can be used as a technique to compromise even a fully patched system.

Security conscious administrators use SSH as their method of interactive remote access. If the version of SSH is current and it is fully patched, the service is generally assumed to be safe. However regardless of whether it is up to date and patched it can still be compromised via brute-force password-guessing attacks. For SSH it is recommended to use public key authentication mechanism to thwart such attacks. For the other interactive services audit passwords to ensure they are of sufficient complexity to resist a brute-force attacks.

### U1.2 Affected Versions

All versions of UNIX/Linux are potentially at risk from improper and default configurations. All UNIX/Linux versions may be affected by accounts having weak or dictionary-based passwords for authentication.

### U1.3 How to determine if you are vulnerable

Default installations (either from the manufacturer or by an administrator) of operating systems or network applications may introduce a wide range of unneeded and unused services. In many cases the uncertainty about operating system or application needs leads many manufacturers or administrators to install all of the software in case it is needed in the future. This simplifies the installation process significantly but also introduces a wide range of unneeded services and accounts that have default/weak/or known passwords.

The use of an updated vulnerability scanner or a port mapper can be highly effective in diagnosing any potential vulnerabilities left by default installations, such as unneeded and/or outdated services/applications. Also, a password cracker can help to avoid the use of weak passwords, which would make more difficult to guess in case of a brute force attack on remote services.

Please note: Never run a password cracker/vulnerability scanner, even on systems for which you have root-like 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.

## U1.4 How to Protect against These Vulnerabilities

### Unnecessary Services

- Scan the server with a port scanner or vulnerability assessment tool to determine what unnecessary services are running on a system. Disable the services that are not required by any necessary applications.
- Install the latest vendor patches regularly to mitigate vulnerabilities in exposed services. Patch management is a critical part of the risk management process.
- Use The Center for Internet Security benchmarks from [www.cisecurity.org](http://www.cisecurity.org) for your OS and services you use. Also consider using Bastille to harden Linux and HP-UX based hosts from [www.bastille-linux.org](http://www.bastille-linux.org).
- Consider moving services from default ports where possible. Automated scanners tend to only scan default ports.
- Utilize a hardware or software firewall to protect required services.
- Ensure services are protected by vendor-supplied security mechanisms (for example SELinux or address space randomization).

### Brute Force Attacks

- Don't use default passwords on any accounts.
- Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.
- Audit to ensure your password policy is being adhered to.
- Limit the number of failed login attempts to exposed services.
- Limit the accounts that can log in over the network; root should not be one of them.
- Employ firewall rules to limit the source of any remote logins.
- Prohibit shared accounts and don't use generic account names like tester, guest, sysadmin, admin, etc.
- Log failed login attempts. A large number of failed logins to a system may require a further check on the system to see if it has been compromised.
- Consider using certificate based authentication.
- If your UNIX system allows the use of PAM authentication modules, implement PAM modules that check for password's strength.
- Firewall services that do not require access to the Internet.

## U1.5 References

### SSH Brute Force Attacks and Counter Measures

- <http://isc.sans.org/diary.php?storyid=1541>
- <http://isc.sans.org/diary.php?storyid=1491>
- <http://isc.sans.org/diary.php?date=2006-08-01>
- [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1094140,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1094140,00.html)

### General UNIX Security Resources

- <http://www.cisecurity.org>
- <http://www.bastille-linux.org>
- <http://www.puschitz.com/SecuringLinux.shtml>

---

## C1 Web Applications

### C1.1 Description

Applications such as Content Management Systems (CMS), Wikis, Portals, Bulletin Boards, and discussion forums are being used by small and large organizations. Every week **hundreds** of vulnerabilities are being reported in these web applications, and are being actively exploited. The number of attempted attacks every day for some of the large web hosting farms range from **hundreds of thousands to even millions**.

All web frameworks (PHP, .NET, J2EE, Ruby on Rails, ColdFusion, Perl, etc) and all types of web applications are at risk from web application security defects, ranging from insufficient validation through to application logic errors. The most exploited vulnerabilities are:

- **PHP Remote File Include:** PHP is the most common web application language and framework in use today. By default, PHP allows file functions to access resources on the Internet using a feature called "allow\_url\_fopen". When PHP scripts allow user input to influence file names, remote file inclusion can be the result. This attack allows (but is not limited to):
  - Remote code execution
  - Remote root kit installation
  - On Windows, internal system compromise may be possible through the use of PHP's SMB file wrappers
- **SQL Injection:** Injections, particularly SQL injections, are common in web applications. Injections are possible due to intermingling of user supplied data within dynamic queries or within poorly constructed stored procedures. SQL injections allow attackers:
  - To create, read, update, or delete any arbitrary data available to the application
  - In the worst case scenario, to completely compromise the database system and systems around it
- **Cross-Site Scripting (XSS):** Cross site scripting, better known as XSS, is the most pernicious and easily found web application security issue. XSS allows attackers to deface web sites, insert hostile content, conduct phishing attacks, take over the user's browser using JavaScript malware, and force users to conduct commands not of their own choosing - an attack known as cross-site request forgeries, better known as CSRF.

- **Cross-site request forgeries (CSRF):** CSRF forces legitimate users to execute commands without their consent. This type of attack is extremely hard to prevent unless the application is free of cross-site scripting vectors, including DOM injections. With the rise of Ajax techniques, and better knowledge of how to properly exploit XSS attacks, CSRF attacks are becoming extremely sophisticated, both as an active individual attack and as automated worms, such as the Samy MySpace Worm.
- **Directory Traversal:** Directory traversal (file access via ".." or many encoded variants) allows attackers access to controlled resources, such as password files, configuration files, database credentials or other files of the attacker's choosing.

## C1.2 How to Determine If You Are at Risk

Web scanning tools can help find these vulnerabilities, particularly if they are known bugs. However, to find all potential vulnerabilities requires a source code review. This should be done by the developers prior to release.

Inspect your web application framework's configuration and harden appropriately.

System administrators should consider scanning web servers periodically with vulnerability scanners, particularly if they run a large diverse range of user supplied scripts, such as a hosting farm. It is impractical for system administrators to perform detailed penetration tests.

## C1.3 How to Protect against Web Application Vulnerabilities

From the PHP system administration and hosting perspective:

- Upgrade to PHP 5.2 as it eliminates many latent PHP security issues and allows for safer API, such as PDO
- Always test and deploy patches and new versions of PHP as they are released
- Frequent web scanning is recommended in environments where a large number of PHP applications are in use
- Consider using the following PHP configuration:
  - register\_globals (should be off, will break insecure apps)
  - allow\_url\_fopen (should be off, will break apps that rely on this feature, but protect against a very active exploit vector)
  - magic\_quotes\_gpc (should be off, will break older insecure apps)
  - open\_basedir (should be enabled and correctly configured)
  - Consider using least privilege execution features like PHPsuexec or suPHP
  - Consider using Suhosin to control the execution environment of PHP scripts
- Use Intrusion Prevention/Detection Systems to block/alert on malicious HTTP requests. Consider using Apache's mod\_security to block known PHP attacks
- As a last resort, consider banning applications which have a track record of active exploitation, and slow response times to fix known security issues.

From the developer perspective:

- If you use PHP, migrate your application to PHP 5.2 as a matter of urgency.
- To avoid the coding issues above:
  - Develop with the latest PHP release and a hardened configuration (see above)
  - Validate all input appropriately
  - Encode all output using htmlentities() or a similar mechanism to avoid XSS attacks
  - Migrate your data layer to PDO - do not use the old style mysql\_\*(\*) functions as they are known faulty
  - Do not use user-supplied input with file functions to avoid remote file inclusion attacks
- Join secure coding organizations, such as OWASP (see references) to boost skills, and learn about

secure coding

- Test your apps using the OWASP Testing Guide with tools like WebScarab, Firefox's Web Developer Toolbar, Greasemonkey and the XSS Assistant

## C1.4 References

OWASP - Open Web Application Security Project

<http://www.owasp.org>

OWASP Testing Guide

[http://www.owasp.org/index.php/OWASP\\_Testing\\_Guide\\_v2\\_Table\\_of\\_Contents](http://www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents)

OWASP Guide - a compendium of secure coding

[http://www.owasp.org/index.php/Category:OWASP\\_Guide\\_Project](http://www.owasp.org/index.php/Category:OWASP_Guide_Project)

OWASP Top 10 - Top 10 web application security weaknesses

[http://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

Suhosin, a Hardened PHP project to control the execution environment of PHP applications

<http://www.hardened-php.net/suhosin/>

PHP Security Features

<http://php.net/features.safe-mode>

---

## C2. Database Software

### C2.1 Description

Databases are a key element of many systems storing, searching or manipulating large amounts of data. They are found in virtually all businesses, financial, banking, customer relationship and system monitoring applications.

Due to the valuable information they store such as personal or financial details, databases are often a target of attack and are of particular interest to identity thieves. Database systems are often very complex, combining the core database with a collection of applications; some supplied by the database vendor, others written in house (such as web applications). A flaw in any of these components can compromise the stored data. The most common vulnerabilities in database systems can be classified as:

- Use of default configurations with default user names and passwords.
- Buffer overflows in processes that listen on well known TCP/UDP ports.
- SQL Injection via the database's own tools or web front-ends added by users.
- Use of weak passwords for privileged accounts

There are many different database systems available. Some of the most common are Microsoft SQL Server (proprietary, runs on Windows), Oracle (proprietary, runs on many platforms), IBM DB2 and IBM Informix (both proprietary, run on multiple platforms), Sybase (proprietary, runs on many platforms), MySQL and PostgreSQL (both open source and available on many platforms).

All modern relational database systems are port addressable, which means that anyone with readily available query tools can attempt to connect directly to the database, bypassing security mechanisms used by the operating system. The commonly used default connections are: Microsoft SQL via TCP port 1433 and UDP port 1434, Oracle via TCP port 1521, IBM DB2 via ports 523 and 50000 up, IBM Informix via TCP ports 9088 and 9099, MySQL via TCP port 3306, and PostgreSQL via TCP port 5432.

Proof of concept exploits for many database flaws are readily available on the Internet. Due to the network connections they provide, databases may suffer from worms. The most infamous of these was the [SQL Slammer worm](#) in 2003. 2005 saw the appearance of the first Oracle worm: "[Voyager](#)". Whilst this did not carry a damaging payload, it demonstrated what could be done if an Oracle database is not protected.

In addition to addressing the specific vulnerabilities mentioned here, administrators concerned with

database security should consider:

- The impact of standards such as the [Payment Card Industry Data Security Standard](#) that may require encryption of some information such as credit card numbers.
- The risks of transferring large quantities of data onto mobile devices: in the last year there have been numerous reports of personal data being lost through the theft of laptops.

## C2.2 Operating Systems Affected

Most database systems, commercial and open source, run on multiple platforms. Issues regularly cover all supported platforms.

## C2.3 CVE Entries

These are the entries released since October 2005. Earlier vulnerabilities can be found in previous editions of the SANS vulnerabilities lists. In many cases reported issues are not flaws in the databases themselves but in applications built around them, e.g. SQL injection into web interfaces; these have not been included here.

### Oracle

[CVE-2005-3641](#), [CVE-2006-0256](#), [CVE-2006-0257](#), [CVE-2006-0258](#), [CVE-2006-0259](#), [CVE-2006-0260](#), [CVE-2006-0261](#), [CVE-2006-0262](#), [CVE-2006-0263](#), [CVE-2006-0265](#), [CVE-2006-0266](#), [CVE-2006-0267](#), [CVE-2006-0268](#), [CVE-2006-0269](#), [CVE-2006-0270](#), [CVE-2006-0271](#), [CVE-2006-0272](#), [CVE-2006-0282](#), [CVE-2006-0283](#), [CVE-2006-0285](#), [CVE-2006-0286](#), [CVE-2006-0287](#), [CVE-2006-0290](#), [CVE-2006-0291](#), [CVE-2006-0435](#), [CVE-2006-0547](#), [CVE-2006-0548](#), [CVE-2006-0549](#), [CVE-2006-0551](#), [CVE-2006-0552](#), [CVE-2006-0586](#), [CVE-2006-1868](#), [CVE-2006-1871](#), [CVE-2006-1872](#), [CVE-2006-1873](#), [CVE-2006-1874](#), [CVE-2006-3698](#).

Note: This list concentrates on the core Oracle database programs. There are vulnerabilities in other applications that form part of the Oracle suite. Oracle releases quarterly Critical Patch Updates (CPU) covering large numbers of issues in the databases and associated applications. The general advice is to work through these CPUs. Due to the way Oracle released information during this reporting period multiple CVE entries may be reporting a single issue.

### MySQL

[CVE-2006-2753](#).

### PostgreSQL

[CVE-2006-2313](#), [CVE-2006-2314](#).

### IBM DB2

[CVE-2005-3643](#), [CVE-2005-4737](#).

### IBM Informix

[CVE-2005-3642](#), [CVE-2006-3854](#), [CVE-2006-3860](#), [CVE-2006-3862](#).

### Microsoft SQL Server

None during this reporting period.

### Sybase

None during this reporting period.

## C2.4 How to Determine If You Are Vulnerable

It is not sufficient to check a simple, manually maintained list of the applications that have been installed! Because databases are often distributed as components of other applications, it is possible for a database to have been installed without administrators realizing it. Databases may therefore remain unpatched or in vulnerable default configurations. This was graphically demonstrated when the SQL Slammer worm attacked the Microsoft Data Access Component (MDAC), which is included in many applications.

Perform a vulnerability scan on systems to determine whether DBMS software is available, accessible and vulnerable. You can use general vulnerability scanners or tools from database vendors such as [MySQL](#)

Network Scanner, Microsoft SQL server tool. The Microsoft Baseline Security Analyzer is also of use for Microsoft SQL Server

## C2.5 How to Protect Against Database Vulnerabilities

- Ensure that all DBMS are patched up to date. Unpatched or outdated versions are likely include vulnerabilities. Check vendor sites for patch information. Remain up to date with the vulnerabilities and alerts announced by the vendors:
  - Oracle Security Alerts (<http://www.oracle.com/technology/deploy/security/alerts.htm> )
  - MySQL (<http://lists.mysql.com/>)
  - PostgreSQL (<http://www.postgresql.org/support/security>)
  - Microsoft SQL (<http://www.microsoft.com/technet/security/bulletin/notify.msp>)
  - IBM DB2 (<http://www-306.ibm.com/software/data/db2/udb/support/>)
  - IBM Informix (<http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg24009130>)
- Ensure that the DBMS and applications have been secured:
  - Remove/change default passwords on the database's privileged and system accounts before deploying the system on the network. Lists of default accounts are readily available on the Internet.
  - Use minimal privileges.
  - Use stored procedures where possible.
  - Remove/disable unnecessary stored procedures.
  - Set length limits on any form fields.
  - See the references section below for several useful resources to help secure DBMS.
- Use firewalls or other network security devices to restrict network access to the ports associated with database services.
- Do not trust user input! Ensure that the applications linked to databases clean all user input at the server side to avoid attacks such as SQL injection (see <http://www.sans.org/rr/whitepapers/securecode/23.php>)

## C2.6 References

### Generic and multiple database resources

- SANS reading room on database security: [http://www.sans.org/rr/catindex.php?cat\\_id=3](http://www.sans.org/rr/catindex.php?cat_id=3)
- DoD database security technical implementation guide: <http://iase.disa.mil/stigs/stig/database-stig-v7r2.pdf>
- <http://www.databassecurity.com/>

### Oracle

- SANS Comprehensive Security Checklist for Oracle: <http://www.sans.org/score/oraclechecklist.php>
- [https://store.sans.org/store\\_item.php?item=80](https://store.sans.org/store_item.php?item=80)
- [http://www.oracle.com/technology/deploy/security/pdf/twp\\_security\\_checklist\\_db\\_database.pdf](http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf)
- CIS benchmark tool: [http://www.cisecurity.org/bench\\_oracle.html](http://www.cisecurity.org/bench_oracle.html)
- <http://www.petefinnigan.com/orasec.htm>
- <http://otn.oracle.com/deploy/security/index.html>
- <http://www.red-database-security.com>

## MySQL

- SecurityFocus step-by-step guide to securing MySQL: <http://www.securityfocus.com/infocus/1726>
- <http://dev.mysql.com/doc/mysql/en/Security.html>

## PostgreSQL Security Guide

- <http://www.postgresql.org/support/security>
- <http://www.postgresql.org/docs/techdocs.53>

## Microsoft SQL Security

- <http://www.microsoft.com/sql/techinfo/administration/2000/security/default.msp>
- <http://www.sqlsecurity.com/>
- CIS SQL Server Benchmark Tool: [http://www.cisecurity.org/bench\\_sqlserver.html](http://www.cisecurity.org/bench_sqlserver.html)

## IBM DB2

- [http://www.net-security.org/dl/articles/Securing\\_IBM\\_DB2.pdf](http://www.net-security.org/dl/articles/Securing_IBM_DB2.pdf)

## IBM Informix

- <http://www.databasesecurity.com/informix.htm>
- <http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.admin.doc/admin197.htm>

## Sybase

- Guide to Sybase security: <http://www.niiconsulting.com/innovation/Sybase.pdf>

---

## C3. P2P File Sharing Applications

### C3.1 Description

Peer to Peer networks consist of collections of computers or “nodes” that simultaneously function as both “clients” and “servers” to achieve a common purpose. The nodes may exchange data, share resources, provide directory services, support communications and provide real time collaboration tools.

A number of control and communication architectures are utilized. Centralized index servers can provide directory services for data and service availability. In fully distributed networks each node helps with the indexing and directory services and is fully equivalent. Hybrid architectures combine the features of both to different degrees and groups of nodes may “elect/promote” certain nodes to act as regional index/directory servers.

Many legitimate applications use P2P. Software tool vendors, including Microsoft and Sun, provide a variety of tools and encourage development of P2P applications. However, like any data transfer tool, P2P applications can be misused or exploited to illegally share copyrighted material, obtain confidential data, expose users to unwanted pornography, violence or propaganda, distribute and execute malware (viruses, spyware, bots, etc.), overload the network, mine usage and behavior patterns and control bots, all of which can create a legal liability. The liability and legal prosecution may not be limited to the perpetrator

and may be extended to the network sponsor, supporters or members.

The P2P networks themselves may be attacked by modifying legitimate files with malware, seeding malware files into shared directories, exploiting vulnerabilities in the protocol or errors in coding, blocking (filtering) the protocol, denial of service by making the network function slowly, spamming and identity attacks that identify network users and harass them. Legal action has been successfully used to shut down some popular networks that were culprits of copyright infringement.

P2P concepts and techniques are evolving and can be found in:

- File sharing networks—whose main goal is to share resources such as storage and bandwidth. These operate through a distributed network of clients, sharing directories of files or entire hard drives of data. Clients participate by downloading files from other users, making their data available to others and coordinating file searches for other users.
- Cloud Computing —(Also called distributed processing, Grid Computing, mesh networks) where “clouds” of computers are deployed to provide a virtual computing environment to accomplish a given task by distributing processing load and data. Cloud Computing brings servers on-line as needed, and the end user does not know where the data resides or executes at any point. In some cases, the application runs on a combination of servers and on the user’s PC. Server clouds can reside physically in large facilities controlled by one organization or they can also reside all over the Internet. Because resizable computing capacity is based on virtual servers the data owner does not really know where his programs and data reside physically.

Most of the P2P programs use a set of default ports but they 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 and encryption to easily bypass corporate restrictions.

### C3.2 Operating Systems Affected

There are versions of P2P software available for all Microsoft Windows operating systems currently in use, along with versions for Linux, MacOS and most Unix-like Operating Systems.

### C3.3 Detecting P2P activity

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 P2P software works with some well known older programs. However, some programs have moved on to using http, https and other ports that commonly need to be passed through firewalls and proxies.
- Application layer monitoring for P2P protocols can identify programs that use commonly allowed ports (53, 80). However, it fails when more malicious programs encrypt the payload.
- Some host based intrusion prevention software and system change auditing tools can prevent the installation or execution of P2P applications along with other malware.
- Pattern matching / behavioral Intrusion Detection systems can identify potential P2P members. Patterns observed include frequency, timing and size of communication bursts.
- Scanning network and PC storage for content commonly downloaded by P2P users, including \*.mp3, \*.wma, \*.avi, \*.mpg, \*.mpeg, \*.jpg, \*.gif, \*.zip, \*.torrent, and \*.exe.
- Changes in network performance may indicate exploding P2P usage, or malware infections.
- Some Firewalls and Intrusion Detection/Prevention products combine detection techniques to detect/prevent P2P traffic from entering or leaving the network.
- For Microsoft Windows machines, SMS can be used to scan for executables that are installed on

workstations. Furthermore, administrators should limit permissions in order to prevent users from installing such software on their workstations.

- Compromised systems that have malware installed via P2P file sharing will display the same symptoms seen when other means of malware distribution are successful.

### C3.4 How to Protect against P2P Software Vulnerabilities

- Standard users should not be permitted to install software. Restrict Administrative and Power User level privileges to support personnel acting in their support capacity. If a user must have Administrative or Power User privileges, create a separate account to be used for his/her daily office functions, internet surfing and on-line communication.
- Use tools such as Microsoft [DropMyRights](#) for securing Web browsers and mail clients.
- In Active Directory environments, Software Restriction Group Policies can be used in order to block known types of binaries from execution.
- Educate users about P2P networks, the dangers of file sharing and company policy.
- Turn on Egress filtering to restrict any ports not required for business purposes, although as more P2P applications move to http and encryption, this will prove less effective.
- Monitor firewall and IDS logs.
- To reduce malware infections which can be spread through numerous applications, use enterprise-wide anti-virus and antispymware products and ensure that updates are performed daily.
- Use host-based firewalls in addition to perimeter firewalls. Windows XP and Windows 2003 include Windows firewall, which provides adequate protection if properly configured. A variety of third-party host based firewalls (ZoneAlarm, Sygate, Outpost) provide additional functionality and flexibility. Windows 2000, XP and 2003 systems can use IPSec policies in order to provide port filtering of unnecessary network traffic over VPN. In Active Directory environments, IPSec policies and Windows Firewall configuration (for Windows XP SP2 and Windows 2003 SP1) can be managed centrally through Group Policies.
- Disable the Simple File Sharing feature of Windows XP if not explicitly required. [Start - Settings - Control Panel - Folder Options - Tab View - Disable (uncheck) setting Use Simple File Sharing - Apply - OK. ]
- Monitor systems for presence of unknown executables and unauthorized modification of system files. Software products like Tripwire or AIDE (there are commercial and open source versions of the product) can be used to detect changes in files.
- Samba-based shares can be configured to run a filter upon opening or saving of files. A filetype detector and alerting system could prove useful to avoid misuse of shares.

### C3.5 References

Wikipedia Peer-to-peer

<http://en.wikipedia.org/wiki/Peer-to-peer>

Department of Justice Cybercrime web site

<http://www.usdoj.gov/criminal/cybercrime>

Other software providers could be held secondarily liable for copyright infringement.

[http://www.usdoj.gov/criminal/cybercrime/2006IPTFProgressReport\(6-19-06\).pdf](http://www.usdoj.gov/criminal/cybercrime/2006IPTFProgressReport(6-19-06).pdf) FBI Education initiative

<http://www.fbi.gov/cyberinvest/cyberedletter.htm>

The Information Factories

[http://www.wired.com/wired/archive/14.10/cloudware\\_pr.html](http://www.wired.com/wired/archive/14.10/cloudware_pr.html)

Mobile Service Clouds: A Self-managing Infrastructure for Autonomic Mobile Computing Services

<http://www.cse.msu.edu/~farshad/publications/conferences/samimi06msc.pdf>

Cyber Security Tip ST05-007 - Risks of File-Sharing Technology

<http://www.us-cert.gov/cas/tips/ST05-007.html>

Risks of P2P File Sharing (Presentation)

<http://www.ftc.gov/bcp/workshops/filesharing/presentations/hale.pdf>

Securing Windows XP Professional in a Peer-to-Peer Networking Environment

[http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/sec\\_winxp\\_pro\\_p2p.mspx](http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/sec_winxp_pro_p2p.mspx)

Identifying P2P users using traffic analysis - Yiming Gong - 2005-07-21

<http://www.securityfocus.com/infocus/1843>

Bot software looks to improve peerage

<http://www.securityfocus.com/news/11390>

Stop the bots

<http://www.securityfocus.com/columnists/398/1>

How to block specific network protocols and ports by using IPSec (MS KB article 813878)

<http://support.microsoft.com/kb/813878>

Using Software Restriction Policies to Protect Against Unauthorized Software

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx>

Availability and description of the Port Reporter tool (MS KB article 837243)

<http://support.microsoft.com/kb/837243>

New features and functionality in PortQry version 2.0 (MS KB article 832919)

<http://support.microsoft.com/default.aspx?kbid=832919>

Log Parser 2.2

<http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx>

Browsing the Web and Reading E-mail Safely as an Administrator (DropMyRights)

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp>

Amazon Cloud Computing goes beta

<http://www.amazon.com/gp/browse.html?node=201590011>

Checkpoint Application Intelligence

[http://www.checkpoint.com/products/downloads/applicationintelligence\\_whitepaper.pdf](http://www.checkpoint.com/products/downloads/applicationintelligence_whitepaper.pdf)

Microsoft site search for peer-to-peer

<http://search.msdn.microsoft.com/search/default.aspx?siteId=0&tab=0&query=peer-to-peer>

Instant-Messaging-and-P2P-Vulnerabilities-for-Health-Organizations

<http://ezinearticles.com/?Instant-Messaging-and-P2P-Vulnerabilities-for-Health-Organizations&id=232800>

Detecting and Understanding Rootkits

<http://www.buanzo.com.ar/sec/Rootkits.html>

Application Layer Packet Classifier for Linux

<http://l7-filter.sourceforge.net/>

---

## C4. Instant Messaging

### C4.1 Description

The widespread use of instant messaging (IM) continues to increase the security risks for both organizations and individual users. While instant messaging can be a very useful communication tool, it is also subject to

many security concerns. Recent attacks include new variations in the establishment and spread of botnets, and the use of compromised instant messaging accounts to lure users into revealing sensitive information. Variants of e-mail worms (such as the Mytob family) have also been spread through the use of instant messaging. The general risk areas related to instant messaging are:

- Malware -- Worms, viruses, and Trojans transferred through the use of instant messaging. Many bots are controlled via IRC channels.
- Information confidentiality -- Information transferred via instant messaging can be subject to disclosure along any part of the process.
- Network -- Denial of service attacks; excessive network capacity utilization, even through legitimate use.
- Application vulnerabilities -- Instant messaging applications contain vulnerabilities that can be exploited to compromise affected systems.

Popular instant message applications include: AOL Instant Messenger (AIM), Gaim, ICQ, Jabber Messenger, Lotus Sametime, Skype, QQ, Windows Live Messenger (WLM), Google Talk, Trillian and Yahoo! Messenger. Instant messaging protocols include: IRC, MSNP, OSCAR, SIMPLE, XMPP and YMSG.

## C4.2 Affected Operating Systems

Instant messaging applications are available for all popular operating systems.

## C4.3 CVE Entries

[CVE-2006-0992](#), [CVE-2006-4662](#), [CVE-2006-5084](#)

## C4.4 How to Protect against IM Vulnerabilities and Unauthorized IM Usage

- Establish policies for acceptable use of instant messaging and ensure that all users are aware of those policies and clearly understand the potential risks.
- Standard users should not be permitted to install software. Restrict Administrative and Power User level privileges to support personnel acting in their support capacity. If a user must have Administrative or Power User privileges, create a separate account to be used for his/her daily office functions, internet surfing and on-line communication.
- Ensure that vendor patches are promptly applied to instant messaging software, interrelated applications, and the underlying operating system.
- Employ antivirus and antispymware products.
- Do not rely on external IM servers for internal use of instant messaging; Provide a commercial grade IM proxy or internal IM server.
- Create secure communications paths when using instant messaging with trusted business partners.
- Appropriately configure intrusion detection/prevention systems. Understand that many instant messaging applications are capable of enabling associated communications to masquerade as otherwise legitimate traffic (e.g. http).
- Consider deploying products specifically designed for instant messaging security.
- Filter all http traffic through an authenticating proxy server to provide additional capabilities of filtering/monitoring instant messaging traffic.
- Block access to known public instant messaging servers that have not been explicitly authorized.

(Note: Offers only partial protection due to the number of potential external servers.)

- Block popular instant messaging ports. (Note: Offers only partial protection, due to the number of potential protocols and associated ports, and the ability of applications to bypass port restrictions.)
- Monitor using an Intrusion Detection/Prevention system for users creating tunnels for IM or bypassing proxies.

## C4.5 References

Phishers hijack IM accounts

[http://news.com.com/Phishers+hijack+IM+accounts/2100-7349\\_3-6126367.html](http://news.com.com/Phishers+hijack+IM+accounts/2100-7349_3-6126367.html)

Rich presence: a new user communications experience

[http://www.alcatel.com/doctypes/articlepaperlibrary/html/ATR2005Q1/ATR2005Q1A17\\_EN.jhtml](http://www.alcatel.com/doctypes/articlepaperlibrary/html/ATR2005Q1/ATR2005Q1A17_EN.jhtml)

Instant messaging: a new target for hackers

[http://www.leavcom.com/ieee\\_july05.htm](http://www.leavcom.com/ieee_july05.htm)

AIM bot creates "fight combos" to spread

<http://www.securityfocus.com/brief/305>

Secure Instant Messaging in the Enterprise

[http://searchsecurity.techtarget.com/tip/0,289483,sid14\\_gci1199405,00.html](http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1199405,00.html)

---

## C5. Media Players

### C5.1 Description

Media players are popularly used and have an install base of millions of systems. Content is downloaded in the form of multimedia files such as movies, video or music. This content is embedded into Web pages, presentations, or integrated into multimedia applications.

Media players can end up on systems through default installations or bundled with other software. Typically browsers are set up to "conveniently" download and open media files without requiring user interaction. They are also downloaded by users on corporate networks to facilitate transfer of multimedia content to their mobile devices.

A number of vulnerabilities have been discovered in various media players over the last year. Many of these vulnerabilities allow a malicious webpage or a media file to completely compromise a user's system without requiring much user interaction. The user's system can be compromised simply upon visiting a malicious webpage. Hence, these vulnerabilities can be exploited to install malicious software like spyware, Trojans, adware or keyloggers on users' systems. Exploit code is publicly available in many instances.

Some of the more popular media players include:

- Windows: Windows Media Player, RealPlayer, Apple Quicktime, Winamp, iTunes
- Mac OS: RealPlayer, Quicktime, iTunes
- Linux/Unix: RealPlayer, Helix Player

### C5.2 Operating Systems Affected

- Microsoft Windows
- Linux/UNIX
- Mac OS X

## C5.3 CVE Entries

### RealPlayer and Helix Player

CVE-2006-1370, CVE-2006-0323, CVE-2005-2922, CVE-2005-4130, CVE-2005-4126, CVE-2005-3677, CVE-2005-2936

### iTunes

CVE-2006-1249, CVE-2005-4092, CVE-2005-2938

### Winamp

CVE-2006-0708, CVE-2005-3188, CVE-2005-2310

### Quicktime

CVE-2006-2238, CVE-2006-1456, CVE-2006-1249, CVE-2005-3713, CVE-2005-3711, CVE-2005-3710, CVE-2005-3709, CVE-2005-3708, CVE-2005-3707, CVE-2005-2340, CVE-2005-4092, CVE-2005-2743

### Windows Media Player

CVE-2006-0025, CVE-2006-0006, CVE-2005-3591

### Macromedia Flash Player

CVE-2005-3591, CVE-2005-2628

## C5.4 How to Determine If You Are Vulnerable

If you run any of these players, and you are not running the most recent version with all applicable patches, you are vulnerable to the associated attacks. Periodic system reviews of installed software can be used to track unintended media player installations as well as rogue user installations.

## C5.5 How to Protect Against Media Player Vulnerabilities

Following are some common approaches to protect against these vulnerabilities:

- Keep the media players updated with all the latest patches. Most players support updating via the help or tools menus.
- Carefully review default installations of operating systems and other products to ensure they do not include unwanted media players. Configure operating systems and browsers to prevent unintentional installation.
- Use Intrusion Prevention/Detection Systems and Anti-virus and Malware Detection Software to block malicious media files.
- On corporate desktops limit installation of user downloaded software whenever possible. This will allow for better patch management and vulnerability management.
- Don't install media players on systems where media is not to be played (e.g. servers)

## C5.6 References

RealNetworks Media Player Products Home Page

[http://www.realnetworks.com/products/media\\_players.html](http://www.realnetworks.com/products/media_players.html)

Security Reports

<http://service.real.com/help/faq/security/>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=40#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=39#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely2>

Helix Player Home Page

<https://player.helixcommunity.org/>

## News, Including Security Announcements

<https://helixcommunity.org/news/>

## Security Reports

<http://www.sans.org/newsletters/risk/display.php?v=4&i=40#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=39#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely2>

## Apple QuickTime Home Page

<http://www.apple.com/quicktime/>

## Apple iTunes Home Page

<http://www.apple.com/itunes/>

## Apple Security Updates

<http://docs.info.apple.com/article.html?artnum=61798>

## QuickTime Support

<http://www.apple.com/support/quicktime/>

## Security Reports

<http://www.sans.org/newsletters/risk/display.php?v=5&i=39#06.39.25>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=37#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=27#06.27.34>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=26#widely4>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=19#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=11#06.11.28>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=2#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=49#05.49.24>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely2>

## Nullsoft Winamp

<http://www.winamp.com/>

<http://www.winamp.com/about/news.php>

## Security Reports

<http://www.sans.org/newsletters/risk/display.php?v=5&i=25#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=8#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely4>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=5#widely1>

## Microsoft Windows Media Player Home Page

<http://www.microsoft.com/windows/windowsmedia/default.aspx>

## Windows Media Player 10 Security

<http://www.microsoft.com/windows/windowsmedia/mp10/security.aspx>

## Microsoft Security Bulletin Search

<http://www.microsoft.com/technet/security/current.aspx>

## Security Reports

<http://www.sans.org/newsletters/risk/display.php?v=5&i=24#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely3>

## Macromedia Flash Player Homepage

<http://www.macromedia.com/software/flashplayer>

## Security Reports

<http://www.sans.org/newsletters/risk/display.php?v=5&i=42&rss=Y#06.42.23>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=37#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=28#widely8>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=19#widely5>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=11#06.11.27>

---

## C6. DNS Servers

### C6.1 Description

The Domain Name System (DNS) is a critical Internet mechanism that primarily facilitates the conversion of globally unique host names into corresponding globally unique Internet Protocol addresses using a distributed database scheme. The DNS relies on a confidence model developed in an era of mutual trust that is vastly different from today's generally hostile Internet. Because of the changed nature of the Internet, the DNS is prone to many types of transaction attacks that take advantage of that trust, including cache poisoning, domain hijacking, and man-in-the-middle redirection.

During the past year, the following types of attacks have been carried out by botnets against DNS servers.

1. **Recursion Denial of Service Attacks:** A Botmaster publishes a large DNS record in a compromised DNS server or in a DNS server set up for this purpose. The botmaster then directs the botnet to send small UDP/53 queries to public recursive name servers with a forged return address pointed at the targeted victim. As a result, the recursive DNS servers, rather than the bots, directly attack the victim. This effect can be amplified further by making the DNS records larger than a typical UDP/53 response packet, thus forcing a TCP/53 transaction.
2. **Spoofing Authoritative zone Answers:** The botmaster establishes a fake web site (phishing site) on a compromised web server. The botmaster then directs the botnet to listen for requests and spoof DNS replies for a particular zone with an answer pointing to the compromised web server. A twist on this attack is to act locally on the bot-infected computer and modify the local hosts file with entries pointing to the fake web site.

### C6.2 How to Determine If You Are at Risk

All Internet users are at risk of having incorrect data being returned from DNS queries. If scanning the DNS servers under your control shows that the current version or patch(es) released by the appropriate DNS software vendor have not been installed, your DNS server(s) are at risk.

A proactive approach to maintaining the security of any DNS server is to subscribe to one of the customized alerting and vulnerability reports, such as those available from SANS, Secunia, and others, or by keeping up with advisories posted at the Open Source Vulnerability Database (<http://www.osvdb.org>). In addition to security alerts, an updated vulnerability scanner can be highly effective in diagnosing any potential vulnerabilities in DNS servers. In addition the DNS server configuration should be reviewed and tested to ensure that inappropriate recursion or updates are not allowed.

### C6.3 How to Protect against DNS Vulnerabilities

As with any software package, updates and patches to DNS server software must be applied as soon as they are available and have been tested for any impact to local network operations.

To protect against DNS vulnerabilities:

- Apply all vendor patches or upgrade DNS servers to the latest version. For more information about hardening a DNS installation, see the articles about securing name services as referenced in [Center for Internet Security DNS BIND benchmark](#) and the appropriate CIS benchmark for the OS platform.
- 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).

- In Unix, to prevent a compromised DNS service from exposing one's entire system, restrict the service so that it runs as a non-privileged user in a chroot()ed directory (jail).
- Do not allow your recursive DNS servers to be used anything other than your own network blocks unless required. Firewalls or DNS configurations files can prevent this in most cases. Disabling recursion and glue fetching assists in defending against DNS cache poisoning.
- Consider signing your entire zone using DNS Security Extensions (DNSSEC).
- On most systems running BIND, the command "named -v" will show the installed 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 two major versions for BIND are 8 and 9. The Internet Systems Consortium recommends that all BIND users migrate to version 9 as soon as possible.
- DNS servers are integrated into many common products such as firewalls, enterprise network servers, and security appliances. All Internet-facing servers, appliances, and systems must be checked to ensure that any embedded DNS software is updated and maintained per the vendor's recommendations.
- Servers that are not specifically designed to support DNS transactions (for example, mail, web, or file servers) should not be running a DNS server application or daemon unless absolutely necessary.

## C6.6 References

### DNS Vulnerabilities

- <http://www.sans.org/newsletters/risk/display.php?v=4&i=11>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=14#widely1>
- <http://isc.sans.org/presentations/dnspoisoning.php>
- <http://thekelleys.org.uk/dnsmasq/doc.html>
- <http://www.icir.org/vern/papers/reflectors.CCR.01/node8.html>

### DNS Version Survey and Server Software

- <http://mydns.bboy.net/survey/>
- <http://www.dns.net/dnsrd/servers/>

### Inner Workings of DNS

- <http://www.internic.net/faqs/authoritative-dns.html>
- <http://www.sans.org/rr/whitepapers/dns/>
- <http://www.cert.org/archive/pdf/dns.pdf>
- <http://www.isc.org/index.pl>
- <http://www.microsoft.com/windows2000/technologies/communications/dns/default.mspix>
- <http://www.dns.net/dnsrd/>

### DNSSEC Deployment

- <http://www.dnssec-deployment.org/>
- <http://www.dnssec.net>
- <http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf>

### DNS Security Best Practices

- <http://www.cymru.com/Documents/secure-bind-template.html>
- <http://www.softpanorama.org/DNS/security.shtml>
- [http://cookbook.linuxsecurity.com/sp/bind\\_hardening8.html](http://cookbook.linuxsecurity.com/sp/bind_hardening8.html)
- <http://www.isc.org/index.pl?sw/bind/bind-security.php>
- [http://www.cisecurity.org/bench\\_bind.html](http://www.cisecurity.org/bench_bind.html)
- [http://www.cert.org/tech\\_tips/usc20\\_full.html](http://www.cert.org/tech_tips/usc20_full.html)

---

## C7. Backup Software

### C7.1 Description

Backup software is a valuable asset for any organization. The software typically runs on a large number of systems in an enterprise. In recent years with the growth in data size, the trend has been to consolidate the backup function into few servers, or even a single server. The hosts requiring the backup service communicate with the backup server over the network. This may be a push where the client sends data to the server or a pull where the server connects to each client in turn, or a combination of both. During the last year a number of critical backup software vulnerabilities have been discovered. These vulnerabilities can be exploited to completely compromise systems running backup servers and/or backup clients. An attacker can leverage these flaws for an enterprise-wide compromise and obtain access to the sensitive backed-up data. Exploits have been publicly posted for some of these flaws, and these vulnerabilities are getting exploited in the wild.

### C7.2 Operating Systems and Backup Software Affected

All operating systems running backup server or client software are potentially vulnerable to exploitation. The affected operating systems are mainly Windows and UNIX systems.

The following popular backup software packages are known to be affected by vulnerabilities

- Symantec Veritas NetBackup/Backup Exec
- Computer Associates BrightStor ARCserve
- EMC Legato Networker

### C7.3 CVE Entries

[CVE-2005-3116](#), [CAN-2005-3659](#), [CAN-2005-3658](#), [CVE-2006-0989](#), [CVE-2006-0990](#), [CVE-2006-0991](#), [CVE-2006-5142](#), [CVE-2006-5143](#)

### C7.4 How to Determine If You Are Vulnerable

- Use any Vulnerability Scanner to detect vulnerable backup software installations.
- If you are using aforementioned backup software, it is recommended to update to the latest version. Monitor your backup software vendor site and subscribe to the patch notification system if they have one, and some of general security related sites such as [US-CERT](#), CERT, SANS ([Internet Storm Center](#)) for new vulnerability announcements relating to your chosen backup software.
- The typical ports used by backup software:
  - Symantec Veritas Backup Exec
    - TCP/10000 TCP/8099, TCP/6106, TCP/13701, TCP/13721 and TCP/13724 (A listing of ports used by Veritas backup daemons is available [here](#))
  - CA BrightStor ARCserve Backup Agent
    - TCP/6050, UDP/6051, TCP/6070, TCP/6503, TCP/41523, UDP/41524
  - Sun and EMC Legato Networker

## C7.5 How to Protect against These Vulnerabilities

- Ensure the latest vendor supplied software patches are installed on the clients and servers.
- The ports being used by backup software should be firewalled from any untrusted network including the Internet.
- Data should be encrypted when stored on backup media and while being transported across the network.
- Host/Network based firewalls should be run to limit the accessibility of a systems backup software to ensure that only the appropriate backup hosts can communicate on the backup server ports
- Segregate your network to create a separate backup network VLAN.
- Backup media should be stored, tracked and accounted like other IT assets to deter and detect theft or loss.
- Backup media should be securely erased, or physically destroyed at the end of its useful life.

## C7.6 References

### Computer Associates Advisories

<http://supportconnectw.ca.com/public/storage/infodocs/basbr-secnotice.asp>

<http://zerodayinitiative.com/advisories/ZDI-06-030.html>

<http://zerodayinitiative.com/advisories/ZDI-06-031.html>

### Symantec Veritas Advisories

<http://seer.support.veritas.com/docs/279553.htm>

<http://support.veritas.com/docs/281521>

<http://www.idefense.com/application/poi/display?id=336&type=vulnerabilities>

<http://www.zerodayinitiative.com/advisories/ZDI-06-005.html>

<http://www.zerodayinitiative.com/advisories/ZDI-06-006.html>

### EMC Legato and Sun Advisories

[http://www.legato.com/support/websupport/product\\_alerts/011606\\_NW.htm](http://www.legato.com/support/websupport/product_alerts/011606_NW.htm)

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0027.html>

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0028.html>

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0029.html>

---

## C8. Security, Enterprise, and Directory Management Servers

### C8.1 Description

Applications such as on-server virus and spam filters, directory servers, and management and monitoring systems pose a unique security challenge; in addition to compromising the system hosting them, they provide opportunities to attack other systems.

### C8.2 Applications Affected

These applications can be divided into multiple categories:

- **Directory Servers** - Used to maintain user and system information. Compromising these applications can give access to large amounts of information, including usernames and (possibly encrypted) passwords.

- **Monitoring Systems** - Used to monitor various other systems. These applications often have user accounts on monitored clients, allowing an attacker easy access to client systems.
- **Configuration and Patch Systems** - These systems are used to maintain client configurations and patches. Compromising these systems provides an easy path to further distribute malware.
- **Spam and Virus Scanners** - Vulnerabilities in these systems can often be exploited with little or no user interaction, by simply sending a specially-crafted email message. Once compromised, attackers can more easily send spam and virus-containing emails. Additionally, these systems often contain vital information, such as users' mailboxes.

These applications tend to run on a variety of operating systems, including common systems such as Microsoft Windows or Solaris, and rarer systems like HP-UX and Novell Netware.

### C8.3 CVE Entries

[CVE-2006-5478](#), [CVE-2006-4509](#), [CVE-2006-4510](#), [CVE-2006-4177](#), [CVE-2006-2496](#), [CVE-2006-0992](#), [CVE-2005-3653](#), [CVE-2005-1928](#), [CVE-2005-1929](#)

### C8.4 How to Determine If You Are at Risk

- Use a vulnerability scanner.
- Track vendor security announcements.

### C8.5 How to Protect Against These Vulnerabilities

- Keep the systems updated with all the latest patches and service packs. If provided, use an automatic update system.
- Use Intrusion Prevention/Detection Systems to prevent/detect attacks exploiting these vulnerabilities.
- Ensure that only authorized users and systems have access to the affected systems.

### C8.6 References

Trend Micro ServerProtect Multiple Vulnerabilities

<http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0066.html>

<http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0067.html>

<http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0068.html>

Trend Micro Home Page

<http://www.trendmicro.com/>

CA iTechnology iGateway Buffer Overflow

[http://supportconnectw.ca.com/public/ca\\_common\\_docs/igatewaysecurity\\_notice.asp](http://supportconnectw.ca.com/public/ca_common_docs/igatewaysecurity_notice.asp)

CA Home Page

<http://www.ca.com/>

Novell eDirectory iMonitor Remote Buffer Overflows

<http://www.zerodayinitiative.com/advisories/ZDI-06-016.html>

Novell Home Page

<http://www.novell.com>

Symantec Sygate Management Server SQL Injection

<http://securityresponse.symantec.com/avcenter/security/Content/2006.02.01.html>

Symantec Home Page

<http://www.symantec.com/>

HP OpenView Multiple Remote Command Execution

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00672314>

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00671912>

HP OpenView Storage Data Protector Remote Code Execution

<http://archives.neohapsis.com/archives/bugtraq/2006-08/0273.html>

HP OpenView Home Page

<http://h20229.www2.hp.com/>

PatchLink Update Server Multiple Vulnerabilities

<http://archives.neohapsis.com/archives/bugtraq/2006-06/0631.html>

PatchLink Home Page

<http://www.patchlink.com/>

Barracuda Spam Firewall Remote Command Injection

<http://archives.neohapsis.com/archives/bugtraq/2006-08/0093.html>

Barracuda Home Page

<http://www.barracudanetworks.com/ns/?L=en>

McAfee ePolicy Orchestrator/ProtectionPilot Remote Buffer Overflow

McAfee Home Page

<http://www.mcafee.com/>

---

# N1 VoIP Servers and Phones

## N1.1 Description

VoIP technology has seen rapid adoption during the past year. At the same time, there has been an increase in security scrutiny of typical components of a VoIP network such as the call proxy and media servers and the VoIP phones themselves. Various products such as [Cisco Unified Call Manager](#), [Asterisk](#) and a number of VoIP phones from various vendors have been found to contain vulnerabilities that can either lead to a crash or a complete control over the vulnerable server/device. By gaining a control over the VoIP server and phones, an attacker could carry out VoIP phishing scams, eavesdropping, toll fraud or denial-of-service attacks.

Since many VoIP servers especially the ones at VoIP service providers are an interface between SS7 (traditional phone signaling) and IP networks, an attacker capable of compromising a vulnerable VoIP server could even potentially manipulate the SS7 signaling interconnection to disrupt services on the Public Switched Telephone Network (PSTN).

## N1.2 CVE Entries

Asterisk

[CVE-2006-2898](#), [CVE-2006-4345](#), [CVE-2006-4346](#), [CVE-2006-5444](#)

Cisco Call Manager

[CVE-2006-0368](#), [CVE-2006-3594](#)

VoIP Phones

[CVE-2005-3717](#), [CVE-2005-3722](#), [CVE-2005-3723](#), [CVE-2006-0305](#), [CVE-2006-0374](#), [CVE-2006-0834](#), [CVE-2006-5038](#)

## N1.3 How to Mitigate These VoIP Vulnerabilities

- Apply the vendor supplied patches for VoIP servers and phone software/firmware.
- Ensure that the operating system running the VoIP server is patched with the latest OS patch supplied by either the OS vendor or the VoIP product vendor.
- Scan the VoIP servers and phones to detect open ports. Firewall all the ports from the Internet that are not required for keeping up the VoIP infrastructure.
- Use a VoIP protocol aware firewall or Intrusion Prevention product to ensure that all UDP ports on VoIP phones are not open to the Internet for RTP/RTCP communications.
- Disable all the unnecessary services on phones and servers (telnet, HTTP etc.)
- Use VoIP protocol fuzzing tools such as [OULU SIP PROTOS Suite](#) against the VoIP components to ensure the VoIP protocol stack integrity.
- Additional caution should be taken at the product selection phase to ensure the VoIP product vendor supports OS patches as they are released. Many VoIP vendors will void support for unapproved patches and may take considerable time before approving them.
- Apply separate VLANs to your voice and data network as much as your converged network will allow. Ensure that VoIP DHCP and TFTP servers are separate from your data network.
- Change the default passwords on phones' and proxies' administrative login functions.

## N1.4 References

Asterisk Vulnerabilities

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

<http://archives.neohapsis.com/archives/bugtraq/2006-06/0139.html>

<http://archives.neohapsis.com/archives/fulldisclosure/2006-08/0617.html>

<http://archives.neohapsis.com/archives/bugtraq/2006-10/0311.html>

Cisco Unified Call Manager Vulnerabilities

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a00805e8a55.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a00805e8a55.shtml)

---

## N2. Network and Other Devices Common Configuration Weaknesses

### N2.1 Description

Network devices, such as routers and switches, often have a reputation for security and stability. Additionally, network-accessible devices such as printers and fax machines are often considered inherently secure. Very often, both classes of devices are omitted from security policies and audits.

Because of the unique role these devices play in network infrastructure, they often have default configurations that emphasize ease of use and configuration, rather than security. This section discusses the common insecurities present in many default configurations of network and network-accessible devices.

### N2.2 Common Default Configuration Issues

#### N2.2.1 Default SNMP Community Strings

Default and often a hard-coded community string continues to be an issue with networking products. This year Cisco IOS versions 12.2 through 12.4 before 20060920 used by certain Cisco devices and a 3Com switch were found vulnerable to this issue.

Example CVEs: [CVE-2006-4950](#), [CVE-2006-5382](#)

#### N2.2.2 Default Accounts, Passwords, Encryption Keys, and Tokens

Many devices are configured with default passwords and other authentication tokens. These often allow complete administrative access to the device. In the case of wireless devices, default encryption keys can make traffic monitoring and sniffing trivially easy.

Example CVEs: [CVE-2006-0789](#), [CVE-2006-0834](#), [CVE-2006-3287](#)

#### N2.2.3 Unnecessary Services

Many devices are configured to run other services in addition to those necessary for the business purpose of the device. For example, many printers provide both HTTP and FTP printing interfaces. These interfaces are often enabled by default. Unnecessary services provide potential security holes, and make logging and administration more difficult.

#### N2.2.4 Unencrypted and Unauthenticated Administration Protocols

Devices are often administered via protocols that do not support encryption or authentication. HTTP and telnet administration interfaces transmit all information in the clear, and TFTP transmits all information in the clear and does not support authentication. Protocols that support encryption and authentication, such as HTTPS and SCP should be used whenever possible.

### N2.3 Vulnerabilities in Printers

Devices such as printers, fax machines, and scanners often contain the configuration weaknesses described above. These devices often go unpatched and can present a significant security risk to an organization.

Example CVEs: [CVE-2006-0788](#), [CVE-2006-2108](#)

### N2.4 How to Protect Against These Vulnerabilities

#### N2.4.1 Perform a Complete Configuration Audit

Storing device configurations in a centralized repository and regularly examining these configurations can make it easy to spot weaknesses. Using a tool such as Cisco's CiscoWorks can aid in configuration management.

CiscoWorks Home Page <http://www.cisco.com/en/US/products/sw/cscowork/ps2425/>

RANCID - Cisco Config Monitoring Tool <http://www.shrubbery.net/rancid>

CISecurity Network Element Benchmarks and Audit Tools <http://www.cisecurity.org>

#### N2.4.2 Set Up a Syslog Server

Many devices support logging via the syslog protocol. Syslog servers are included by default on all Unix, Unix-like, and Linux systems, and free syslog servers are available for Microsoft Windows. Properly configured logging on a network device will allow the syslog server to log accesses to the device, any modification to the configuration as well as any policy violations enforced by the device.

Configuring Cisco Syslog <http://www.linuxhomenetworking.com/cisco-hn/syslog-cisco.htm>

Central Loghost Mini-HOWTO <http://www.campin.net/newlogcheck.html>

### N2.4.3 Disable Default Accounts and Change Default Passwords

Any default accounts should be disabled, and all default passwords and other authentication tokens should be changed to secure alternatives. Cisco SNMP Community Strings [http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd\\_technology\\_support\\_sub-protocol\\_home.html](http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html)

### N2.4.4 Disable Unnecessary Services

Any services that are not needed should be disabled. Any necessary services should, if possible, be restricted to authenticated users.

Cisco TCP and UDP Small Services [http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products\\_tech\\_note09186a008019d97a.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a008019d97a.shtml)

### N2.4.5 Use Encrypted and Authenticated Administration Protocols

If the device supports administration via HTTPS or SSH, these are preferable to unencrypted protocols such as HTTP or telnet. For file transfer, SCP, HTTPS, or FTPS should be preferred over TFTP or FTP. Strong passwords or other strong authentication methods should always be used.

Configuring SSH on Cisco Devices

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800ca7d5.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html)

### N2.4.6 Use Port-Level Security

If your network infrastructure supports it, implement port-level security on switches. This can help prevent rogue systems connecting to the network, and can help contain and detect ARP spoofing and other attacks.

Configuring Port Level Security on Cisco Devices

<http://articles.techrepublic.com.com/5100-1035-6123047-1.html>

<http://articles.techrepublic.com.com/5100-1035-6123047-2.html>

---

## H1. Excessive User Rights and Unauthorized Devices

### H1.1 Introduction

Some attacks cannot be effectively prevented by technical controls alone. Unwary users can be enticed to do unsafe things. Clever users can find unsafe ways to get things done, unintentionally exposing the company to attack. To protect against attacks exploiting these weaknesses, administrative controls supplement technical and physical controls.

In time, technical controls may be able to enforce policies that proscribe user behavior. In the mean time, to make those administrative controls effective, organizations need to trust but verify to identify policy violations so corrective action can be taken. Enforcement (i.e. a process to bring systems back into compliance with policy whenever violations are detected) is also essential.

#### H.1a Unauthorized and/or infected devices on network

The best efforts to secure an information system are futile if unauthorized devices are allowed to connect to the network. A rogue wireless access point can be an open door to a hacker. A personal laptop that is brought into the office can introduce whatever malware it has collected into the corporate network. An unprotected company laptop that has been connected to an unsafe public network will eventually bring back all the malware it has collected to be shared with the entire company. A router or PC secretly connected to an open ethernet port by a visitor can give him a private, open back door into the company network. A USB flash drive carrying a virus can infect a machine simply by plugging it in.

At the same time, networks administrators must take care of users who return to corporate or private networks. Policies can tell users what is authorized, but testing and network access control can ensure the policies are being followed.

Continuous data flow monitoring can immediately identify unauthorized devices. In addition, network access control systems can scan company laptops for viruses, trojans, spyware, and adware to reveal hidden vulnerabilities brought into the network from the outside. They can then segregate vulnerable systems, and correct the problem, and then allow them appropriate access rights.

#### H.1b Excessive User Rights and Unauthorized software

Unmanaged software introduces multiple risks for the corporation. That software may contain security vulnerabilities, and users may not be sufficiently diligent about applying patches. Sometimes users may install software which, unknown to them, contains malware which could compromise the entire network. Also, sometimes users may install software providing functionality (eg. P2P) that invites new vulnerabilities into the network. Those who are responsible for securing networks should consider implementing policies, and associated detective and corrective controls, to mitigate this class of vulnerabilities.

You are vulnerable if your users can install their own software, and you have not taken steps to control that process.

The key control that protects against this set of problems is a fully enforced policy of limiting user rights. If users can install software

without authorization, than malware that gets on those systems can also install software. Additionally, lists of authorized software (white lists) help limit problems, as long as all systems are checked for unauthorized software when they connect to the corporate network.

## H1.2 References

<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17170&TEMPLATE=/ContentManagement/ContentDisplay.cfm>

[http://www.techweb.com/wire/security/20020904\\_security](http://www.techweb.com/wire/security/20020904_security)

<http://technet2.microsoft.com/WindowsServer/en/library/e903f7a2-4def-4f5f-9480-41de6010fd291033.msp?mfr=true>

[http://www.sans.org/resources/policies/Password\\_Policy.pdf](http://www.sans.org/resources/policies/Password_Policy.pdf)

[http://www.sans.org/resources/policies/Acceptable\\_Use\\_Policy.pdf](http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf)

<http://www.cerias.purdue.edu/weblogs/spaf/general/post-30/>

<http://www.csoonline.com/caveat/062306.html>

---

## H2. Users (Phishing/Spear Phishing)

### H2.1 Description

The word "phishing" was first used around 1996 when hackers began stealing America On-Line accounts by sending email to AOL users that appeared to come from AOL. Phishing attacks now target users of online banking, payment services such as PayPal, and online e-commerce sites. Phishing attacks are growing quickly in number and sophistication. In fact, since August 2003, most major banks in the USA, the UK and Australia have been hit with phishing attacks.

#### Password/PIN Phishing

Phishers send email to get you to go to a web site where you are fooled into exposing your banking information so they can take the money in your account. They can also use that technique to get data on your online accounts such as Hotmail, Yahoo, and eBay. Once they have your user name and password, the phishers will attempt to obtain a victims billing information. Once someone gets into your eBay account, for example, they have access to your past and current transactions, personal information such as your PayPal billing information, and your physical address.

#### VoIP phishing

A newer form of phishing replaces a web site with a telephone number. In this form of phishing, an email tells you to call a specific number where an audio response unit, at the end of a compromised VoIP phone line, waits to take your account number, personal identification number, password, or other valuable personal data. The person/audio unit on the other end of the VoIP phone line might claim that your account will be closed or other problems could occur if you don't respond.

#### Spear Phishing

Spear phishing is a highly targeted phishing attack. Spear phishers will send e-mail that includes information about staff or current organizational issues that make it appear genuine to employees or members within a certain company, government agency, organization, or group. The message may look like it comes from your employer or from a colleague who might send an e-mail message to everyone in the company, such as the head of human resources or the person who manages the computer systems, and could include requests for user names or passwords. Spear phishing has become one of the most damaging forms of attacks on military organizations in the US and other developed countries. Attackers gain user name and password information and then break in to exfiltrate sensitive military information.

### H2.1 How to Prevent Phishing Attacks

The most promising method of stopping spear phishing is continuous periodic exercises for all your users in which they experience safe phishing. A child often learns not to touch a stove after he has burnt his finger. By making the phishing experience illuminating, but not too painful, you can get the same effect without doing real damage.

A second defense is universal two-factor authentication. If your organization is not economically strong and cannot afford two-factor authentication, another method used to prevent phishing and other types of comprises is the implementation of verification tools such as secret images, and or challenge questions. Secret Images works by having a user select one or more images in advance. The images is only known to the customer and the authenticator, the process works by showing this images to the end user, the end user should be instructed that when this image is not present the site is NOT legitimate and to contact a customer service rep as soon as possible. Challenge Questions work by having a user select multiple secret questions in advance, that only the customer and the authenticator are aware of. When authenticating the users are then challenged and respond with the predefined answers.

Less effective, but still valuable methods include

- Do not mass e-mail your customer base with web links directed to your site or any other website. Doing so teaches your customer base to accept web link opening, and to assume trust. This will open you up for Phishing attacks in the future.

- Do not use your authentication credentials, or other Non-public personal information to authenticate your customer base. (e.g. ATM Pin or Social Security numbers used as the password for your online web portal.)
- Log information such as IP address, location information, and computer finger prints to uniquely track any device accessing changing customers data online.
- Be sure to report all incidents of fraud to a law-enforcement agency so that the data can be correlated with other attacks for attack and incident pattern matches.
- **Anti-Phishing Software:** Applications that attempt to identify Phishing content in both e-mail and web sites usually integrates with Web Browsers and e-mail clients, in the form of a toolbar that displays the real domain name of the website the viewer is about to visit or is currently visiting in an attempt to prevent fraudulent activity. Several software options exist as either as a built in software feature or a plug-in for both Firefox and Internet Explorer.
  - Microsoft IE 7
  - NetCraft Toolbar: available for both Internet Explorer and Firefox
  - Google Safe browsing: available for Firefox
  - Ebay Toolbar: available for Internet Explorer
  - Earthlink Scamblocker: available for both Internet Explorer and Firefox
  - Geotrust Trustwatch - available for Internet Explorer, Firefox, and Flock
- **User Education** One of the best strategies to combat Phishing is to educate your users of current and all new phishing attack methods, make them knowledgeable on what to do in the event of a phishing attack. Educate your users who are contacted about customer's accounts. Educate your customers that they should contact your Hotline in the event they are asked for any personal information. Users should be told to type the direct URL of your web portal in to the address bar every time they visit your site to reduce the risk of following a fraudulent link, especially when asked via e-mail.
- **Two Factor / Two way authentication:** While no one prevention method is totally infallible another preferred technological method used to prevent phishing and other types of comprises is the implementation of verification tools such as secret images, and or challenge questions. Secret Images works by having a user select one or more images in advance. The images is only known to the customer and the authenticator, the process works by showing this images to the end user, the end user should be instructed that when this image is not present the site is NOT legitimate and to contact a customer service rep as soon as possible. Challenge Questions work by having a user select multiple secret questions in advance, that only the customer and the authenticator are aware of. When authenticating the users are then challenged and respond with the predefined answers.

## H2.2 References:

AntiPhishing Working Group

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

<http://www.3sharp.com/projects/antiphishing/gonephishing.pdf>

VoIP Phishing Scams

<http://blogs.pcworld.com/staffblog/archives/001921.html>

---

## Z1: Special Section: Zero Day Attacks and Prevention Strategies

### Z1.1 Description

While the risks of zero day vulnerabilities in popular applications and subsequent exploitation have been discussed for several years, zero day attacks saw a significant upward trend in 2006. A zero day vulnerability occurs when a flaw in software code has been discovered and exploits of the flaw appear before a fix or patch is available. If a working exploit of the vulnerability is released into the wild, users of the affected software are exposed to attacks until a software patch is available or some form of mitigation is taken by the user. Mitigation and protection steps are explained later in this section.

### Z1.2. Affected OSs

All operating systems and all software applications are vulnerable to zero day vulnerability discovery and exploitation. While the target of most of the attacks this year were Microsoft products, Apple suffered from several zero day exploits as well. Other than

Apple's OS X, no zero day attacks were reported for Linux, BSD, or other Unix-based operating systems.

### Z1.3. CVE Entries

This past year several vulnerabilities had public exploits available before the official patch or remedy was issued. Some example CVE entries that reflect this trend are:

- Windows Graphical Device Interface Library (.wmf) [CVE-2005-4560](#)
- Microsoft Internet Explorer [CVE-2006-1245](#)
- Microsoft Internet Explorer [CVE-2006-1359](#)
- Microsoft Internet Explorer [CVE-2006-1388](#)
- Microsoft Internet Explorer [CVE-2006-3280](#)
- Microsoft Internet Explorer [CVE-2006-3281](#)
- Microsoft Internet Explorer [CVE-2006-4777](#)
- Apple OS X [CVE-2006-1982](#)
- Apple OS X [CVE-2006-1983](#)
- Apple Safari [CVE-2006-1986](#)
- Apple Safari [CVE-2006-1987](#)
- Microsoft Word [CVE-2006-2492](#)
- Microsoft Excel [CVE-2006-3086](#)
- Microsoft PowerPoint [CVE-2006-3590](#)
- Microsoft PowerPoint [CVE-2006-4694](#)
- Microsoft PowerPoint [CVE-2006-5296](#)
- Microsoft Windows Help File Viewer [CVE-2006-4138](#)
- Microsoft Internet Explorer and Outlook [CVE-2006-4868](#)
- Microsoft Visual Studio [CVE-2006-4704](#)
- Microsoft XML HTTP ActiveX [CVE-2006-5745](#)

### Z1.4. How to Protect against the vulnerabilities

Protecting against zero day vulnerability exploitation is a matter of great concern for most system administrators. To reduce the impact of a zero day attack, follow best business practices such as:

- Adopt a deny-all stance on firewalls and perimeter devices that protect internal networks
- Separate public-facing servers from internal systems
- Turn off unneeded services and remove user applications that do not support operational needs
- Follow the Principle of Least Privilege in setting user access controls, permissions, and rights
- Restrict or limit the use of active code such as Java script or ActiveX in browsers
- Educate users about opening unsolicited file attachments
- Disable the ability to follow links in email
- Disable the ability to automatically download images from the web in email
- Maintain an aggressive in-house security alerting and warning service (or outsource the capability) to become aware of zero-day exploits as they become public.
- Use end-point management solutions to rapidly issue patches or workarounds as they become available
- If you use Microsoft's Active Directory, take maximum advantage of Group Policy Objects to control user access
- Do not rely on antivirus protection alone since zero-day attacks are often not detectable until new signatures are released
- Use third-party buffer overflow protection where possible on all systems

- Follow vendor recommendations on workarounds and mitigations until a patch is available

---

## The Experts Who Helped Create The Top-20 2006 List

- Project Manager and Editor: Rohit Dhamankar, TippingPoint, a division of 3Com
- Adam Safier, Global Systems & Strategies, Inc.
- Alan Rouse, Security Architect, TANDBERG Television
- Alexander Kotkov, UBS Investment Bank
- Amol Sarwate, Manager of Vulnerability Lab, Qualys
- Andrew van der Stock, Director, OWASP
- Anton Chuvakin, Director of Product Management @ LogLogic
- Anthony Richardson, Monash University, Australia
- Arturo "Buanzo" Busleiman - Consultor Independiente en Seguridad, Argentina
- Cesar Tascon Alvarez, Ernst and Young, Spain
- Christopher Bream, PricewaterhouseCoopers
- Chris Riley, Spherion
- Christopher Rowe, Guilford Technical Community College
- Ed Fisher, Ingersoll Rand
- Gerhard Eschelbeck, CTO, Webroot
- David Damato, PricewaterhouseCoopers
- Donald Smith, Qwest
- Edward Ray, Netsec Design and Consulting
- James King, TippingPoint, a division of 3Com
- Jean-Francois Legault, Deloitte & Touche LLP
- Jeff Pike, Integrated Team Solutions Facility
- John-Thomas Gaietto
- John Tannahill
- Johannes Ullrich, Internet Storm Center, SANS
- Jonathan Rubin, Dominion
- Kevin Hong, Korea Information Security Agency (KISA) and KrCERT/CC
- Koon Yaw Tan, Infocomm Development Authority of Singapore
- Leo Pastor, Advanced Consulting and Training, Argentina and Brazil
- Marcos A. Ferreira Jr., NX Security, Brazil
- Marcus Sachs, SRI International and Internet Storm Center, SANS
- Mark J Cox, RedHat
- Mark Goudie, Data Networking Services, Australia
- Matteo Shea, Senior Security Engineer, Communication Valley S.p.a
- Michel Cusin, Bell Security Solutions, Canada
- Michele Guel, Cisco Systems
- Miguel Guirao, Telcel
- Olivier Devaux, vulnpedia.com
- Pedro Bueno - McAfee AvertLabs
- Rajesh Mony, Webroot
- Ralf Durkee, Security Consultant
- Rhodri Davies, Vistorm, UK
- Richard Bejtlich, Taosecurity
- Rick Wanner, Technical Analyst, Corporate Security, SaskTel

- Robert Baskerville, Vistorm, UK
- Pedro Paulo Ferreira Bueno, Brasil Telecom
- Sandeep Dhameja, Ambiron Trustwave
- Syed Mohamed

#### Agencies

- Department of Homeland Security (DHS)
- Computer Emergency Response Team (CERT)
- National Infrastructure Security Coordination Centre (NISCC, UK)
- Computer Emergency Response Team, Canada

---

## SANS Top-20 2006 FAQ

By Rohit Dhamankar, Top 20 Project Director

### For whom is the list written?

Over the past few years, it has become clear to me that the SANS Top-20 list is used by very diverse organizations. Some large organizations use the Top-20 list for double-checking their ongoing security efforts whereas some small organizations use this list exclusively to guide their entire vulnerability remediation effort. So, while creating the list, we tried to serve the diverse audiences.

### Is it still relevant to publish this document in 2006 for a year's worth of vulnerabilities?

Examining the following facts, the answer is a clear "yes".

- Internet scanning data shows that there are still systems facing the Internet that are not patched for vulnerabilities being exploited widely. I, for one, will give up working on this project when I no longer see any Blaster or Slammer worm events triggering on any IDS/IPS in the customer networks.
- Even if all the patches have been applied, there are still zero-days to deal with! This year's list includes a list of defenses for zero-days.
- Security professionals get so focused on the "challenge of the day" that they need reminders, from time to time, of the emerging threats so they can ask for resources to fight those new threats.

### Why do you call it the Top 20 when the number of actual vulnerabilities (CVE's) is much greater than 20.

- Life would be much simpler if one could list 20 critical CVE numbers and say that protecting against attacks using those vulnerabilities would make the Internet safe. The reality, we all know, is far from that. If one just takes the weekly onslaught of web application vulnerabilities for the past year, the number of critical vulnerabilities is well over 100! These are the vulnerabilities that result in hundreds of thousands of attempted web attacks everyday. The Top-20 approach is to help people focus on "classes" of vulnerabilities being exploited, and provide guidance to the system administrators, programmers, and CIOs on how to mitigate each class of flaws.
- The Top-20 groups critical vulnerabilities into classes so that common mitigation strategies can be applied to protect from an entire class. For instance, a large number of MS-RPC overflows can be prevented by blocking the ports 139/tcp and 445/tcp at the network perimeter.
- The Top-20 also helps identify the propagation vectors used by a large number of malware. It is still sad to see in 2006 malware successfully propagating in networks by brute-forcing passwords!
- Finally, the challenge of identifying the vulnerability classes is not a "cookie cutter" problem. There are platforms like Mac OS that use a number of UNIX packages; however, Apple issues patches for the UNIX-inherited packages along with other Mac OS X issues. As a result, a large number of vulnerabilities of varying severities are included in one Apple patch. The recommendation, which sounds trivial, is to apply all the patches. However, at the same time, it is definitely worth pointing out emerging exploit techniques for such platforms with its own class!

If you like you can start calling the list "The SANS Top 20 Attack Target Classes" or "The SANS Top 20 Vulnerability Groups." We've decided to call it The SANS Top 20.

If you have any comments, please write back to [top20@sans.org](mailto:top20@sans.org)

---

#### 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

**SANS**  
**CYBER**  
**DEFENSE**  
**INITIATIVE**  
EAST 2006  
Washington, DC  
December 9-16



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