The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus

Version 6.0 November 22, 2005 Copyright (C) 2005, SANS Institute
Questions / comments may be directed to top20@sans.org.
To link to the Top 20 List, use the SANS Top 20 List logo at www.sans.org/top20/top20logo03.gif

-----Jump To Index of Top 20 Threats -----

Introduction

The SANS Top 20 Internet Security Vulnerabilities

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

This SANS Top-20 2005 is a marked deviation from the previous Top-20 lists. In addition to Windows and UNIX categories, we have also included Cross-Platform Applications and Networking Products. The change reflects the dynamic nature of the evolving threat landscape. Unlike the previous Top-20 lists, this list is not "cumulative" in nature. We have only listed critical vulnerabilities from the past year and a half or so. If you have not patched your systems for a length of time, it is highly recommended that you first patch the vulnerabilities listed in the Top-20 2004 list.

We have made a best effort to make this list meaningful for most organizations. Hence, the Top-20 2005 is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts. They come from the most security-conscious government agencies in the UK, US, and Singapore; the leading security software vendors and consulting firms; the top university-based security programs; many other user organizations; and the SANS Institute. A list of participants may be found at the end of this document.

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

Top Vulnerabilities in Windows Systems

W1. Windows Services
W2. Internet Explorer

PDF | Printer Friendly Version >>

Related Resources

- Press Release (2005-11-22)

Top 20 Archive

- November, 2005 - Version 6 (Current)
- October, 2004 - Version 5
- October, 2003 - Version 4
- October, 2002 - Version 3
- May, 2001 - Version 2
- June, 2000 - Version 1 (Original Top 10)

Upcoming Conferences

- San Diego, CA - Dec. 4, 05
- Toronto, Canada - Dec. 12, 05
- San Francisco, CA - Jan. 13, 06
- Sydney, Australia - Jan. 16, 06
- Phoenix, Arizona - Jan. 30, 06
- Philadelphia, PA - Jan. 30, 06
- Whippany, NJ - Jan. 30, 06
- Phoenix, AZ - Jan. 30, 06
- Brisbane, Australia - Jan. 30, 06
- Columbus, OH - Feb. 6, 06
- Sacramento, CA - Feb. 6, 06
- Tokyo, Japan - Feb. 13, 06
- Ottawa, ON - Feb. 13, 06
- Columbia, MD - Feb. 13, 06
- Orlando, FL - Feb. 24, 06
- Orlando, FL - Mar. 1, 06
- Monterey, CA - Mar. 16, 06
- Honolulu, HI - Mar. 19, 06
- Stay Sharp Program
- SANS On Demand
- SANS@Home
- Mentor Program
- Security Awareness Training

W3. Windows Libraries
W4. Microsoft Office and Outlook Express
W5. Windows Configuration Weaknesses

Top Vulnerabilities in Cross-Platform Applications

C1. Backup Software
C2. Anti-virus Software
C3. PHP-based Applications
C4. Database Software
C5. File Sharing Applications
C6. DNS Software
C7. Media Players
C8. Instant Messaging Applications
C9. Mozilla and Firefox Browsers
C10. Other Cross-platform Applications

Top Vulnerabilities in UNIX Systems

U1. UNIX Configuration Weaknesses
U2. Mac OS X

Top Vulnerabilities in Networking Products

N1. Cisco IOS and non-IOS Products
N2. Juniper, CheckPoint and Symantec Products
N3. Cisco Devices Configuration Weaknesses

Top 20 List v6 Update Log

- No Updates At This Time

Top 20 Translations

Contact top20@sans.org to collaborate in the translation of the Top 20 to your own language.

Top Vulnerabilities in Windows Systems

W1. Windows Services

W1.1 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 functionalities are one of the most common avenues for exploitation.

Remotely exploitable buffer overflow vulnerabilities continue to be the number one issue that affects Windows services. 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. Windows also contains several services which implement network interfaces based on a variety of other protocols, including several Internet standards such as SMTP, NNTP etc. Many of these services can be exploited via anonymous sessions (i.e. sessions with null username and password) to execute arbitrary code with "SYSTEM" privileges.

Earlier versions of the operating system, especially Windows NT and Windows 2000, enabled many of these services by default for 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:

- MSDTC and COM+ Service (MS05-051)
- Print Spooler Service (MS05-043)
- Plug and Play Service (MS05-047, MS05-039)
- Server Message Block Service (MS05-027, MS05-011)
- Exchange SMTP Service (MS05-021)
- Message Queuing Service (MS05-017)
- License Logging Service (MS05-010)
- WINS Service (MS04-045)
- NNTP Service (MS04-036)
- NetDDE Service (MS04-031)
- Task Scheduler (MS04-022)

Exploit code is available for most of these vulnerabilities and has been seen in the wild. Zotob worm and its variants exploited the buffer overflow in Plug and Play service. Note that the patches MS05-047 and MS05-027 replace MS05-039 and MS05-011 respectively.

W1.2 Operating Systems Affected

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-2005-2120, CVE-2005-2119, CVE-2005-1984, CVE-2005-1983, CVE-2005-1978, CVE-2005-1206, CVE-2005-0045, CVE-2005-0560, CVE-2005-0059, CVE-2005-0050, CVE-2004-0567, CVE-2004-1080, CVE-2004-0574, CVE-2004-0206, CVE-2004-0212

W1.4 How to Determine If You Are at Risk

- Use any Vulnerability Scanner
- 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 the **Start->Run** menu by typing **services.msc**. The column "Start Type" shows if the service is configured for start or "disabled". The "Status" column in the UI shows if a service is currently running.

W1.5 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.
- Determine if the vulnerability exists in a non essential component that can be removed. For example if your environment does not require message queuing services (CVE-2005-0059), it can be removed using **control panel -> add remove programs -> windows components** interface. Please take caution when determining this as it could break functionality if there is other software that depends on this.
- In some cases, exposure to the vulnerability could be removed by disabling the corresponding service. For example License Logging Service (CVE-2005-0050) could be disabled in many environments. Type **services.msc** in the **start->run** menu to invoke the service manager interface. Locate the required service and right click after highlighting 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. For example the spools vulnerability (CVE-2005-1984) could be mitigated on Windows 2000 by removing SPOOLSS from the registry value HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes. 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 (CVE-2005-1984, CVE-2005-1983, CVE-2005-1206, CVE-2005-0045 etc) are found on interfaces offered through CIFS, and blocking ports 139 and 445 at the perimeter is essential for preventing remote attack scenarios. 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. (Ex: Message Queue CVE-2005-0059).
- XP SP2 and Windows 2003 SP1 comes with several security enhancements, including the Windows firewall. It is highly advisable to upgrade to these service packs and enable the Windows firewall.

W1.6 References

http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx
http://www.microsoft.com/windows2000/en/advanced/help/sag_TCPIP_ovr_secfeatures.htm
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/4dbc4c95-935b-4617-b4f8-20fc947c7288.mspx

a. Remote Code Execution in MSDTC and COM+ Services
   http://www.microsoft.com/technet/Security/bulletin/ms05-051.mspx
   http://www.sans.org/newsletters/risk/display.php?v=4&i=41#widely2
b. Remote Code Execution in Print Spooler Service
   http://www.microsoft.com/technet/Security/bulletin/ms05-043.mspx
   http://www.sans.org/newsletters/risk/display.php?v=4&i=32#widely3
c. Remote Code Execution in Plug and Play Service
   http://www.microsoft.com/technet/Security/bulletin/ms05-047.mspx
   http://www.microsoft.com/technet/Security/bulletin/ms05-039.mspx

http://www.microsoft.com/security/incident/zotob.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=41#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=43#exploit1
http://www.sans.org/newsletters/risk/display.php?v=4&i=32#widely1
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=7&issue=47#305

d. Remote Code Execution in Server Message Block Service
http://www.microsoft.com/technet/security/bulletin/ms05-027.mspx
http://www.microsoft.com/technet/security/bulletin/ms05-011.mspx
http://www.qualys.com/research/alerts/view.php/2005-06-14
http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely3
http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely6
e. Remote Code Execution in Exchange SMTP Service
http://www.microsoft.com/technet/security/Bulletin/MS05-021.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=15#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=16#exploit1
f. Remote Code Execution in Message Queuing Service http://www.microsoft.com/technet/security/bulletin/ms05-017.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=15#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=19#exploit2
http://www.sans.org/newsletters/risk/display.php?v=4&i=26#exploit2
g. Remote Code Execution in License Logging Service
http://www.microsoft.com/technet/security/bulletin/ms05-010.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=11#exploit1
h. Remote Code Execution in WINS Service
http://www.microsoft.com/technet/security/bulletin/MS04-045.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=48#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=50#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=1#exploit1
http://www.sans.org/newsletters/risk/display.php?v=4&i=2#exploit2
i. Remote Code Execution in NNTP Service
http://www.microsoft.com/technet/security/bulletin/MS04-036.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely2
j. Remote Code Execution in NetDDE Service
http://www.microsoft.com/technet/security/bulletin/MS04-031.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely4
k. Remote Code Execution in Task Scheduler
http://www.microsoft.com/technet/security/bulletin/ms04-022.asp
http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely1

W2. Internet Explorer

W2.1 Description

Microsoft Internet Explorer is the most popular browser used for web surfing and is installed by default on each Windows system. Internet Explorer contains 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.

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 **0-days** i.e. no patch was available at the time the vulnerabilities were publicly disclosed.

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

a. Cumulative Security Update for Internet Explorer (MS05-052)
b. Cumulative Security Update for Internet Explorer (MS05-038)
c. JView Profile Remote Code Execution (MS05-037)
d. Cumulative Security Update for Internet Explorer (MS05-025)
e. Cumulative Security Update for Internet Explorer (MS05-020)
f. Cumulative Security Update for Internet Explorer (MS05-014)
g. Windows Shell Remote Code Execution (MS05-008)
h. Cumulative Security Update for Internet Explorer (MS04-040)
i. Cumulative Security Update for Internet Explorer (MS04-038)
j. Cumulative Security Update for Internet Explorer (MS04-025)

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

W2.2 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.

W2.3 CVE Entries

CVE-2003-1048, CVE-2004-0216, CVE-2004-0549, CVE-2004-0566, CVE-2004-0727, CVE-2004-0841, CVE-2004-0842, CVE-2004-0843, CVE-2004-0844, CVE-2004-1050, CVE-2005-0053, CVE-2005-0054, CVE-2005-0055, CVE-2005-0056, CVE-2005-0553, CVE-2005-0554, CVE-2005-0555, CVE-2005-1211, CVE-2005-1988, CVE-2005-1989, CVE-2005-1990, CVE-2005-2087, CVE-2005-2127

W2.4 How to Determine If You Are at Risk

- Use any Vulnerability Scanner.

W2.5 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.
- Keep the systems updated with all the latest patches and service packs. If possible enable Automatic Updates on all systems.
- To prevent exploitation of remote code execution vulnerabilities at Administrator level, users' tools like Microsoft DropMyRights can be used to implement "least privileges" for Internet Explorer.
- Many spyware programs are installed on a system as a 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 by AV scanners. Another choice is to periodically review your BHOs using BHO-Daemon or Microsoft AntiSpyware.
- Use Intrusion Prevention/Detection Systems and Anti-virus and Malware Detection Software to block malicious HTML script code.

W2.6 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.
- Please also ensure that no un-trusted sites are in the Trusted sites or Local intranet zones as these zones have weaker security settings than the other zones

W2.7 References

Internet Explorer Security Updates

a. http://www.microsoft.com/technet/security/Bulletin/MS05-052.mspx
   http://www.sans.org/newsletters/risk/display.php?v=4&i=41#widely3
b. http://www.microsoft.com/technet/security/Bulletin/MS05-038.mspx
   http://www.sans.org/newsletters/risk/display.php?v=4&i=32#widely2
c. http://www.microsoft.com/technet/security/Bulletin/MS05-037.mspx
   http://www.sans.org/newsletters/risk/display.php?v=4&i=28#widely1
d. http://www.microsoft.com/technet/security/Bulletin/MS05-025.mspx
   http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely1

e. http://www.microsoft.com/technet/security/Bulletin/MS05-020.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=15#widely3
http://www.sans.org/newsletters/risk/display.php?v=4&i=17#exploit2
f. http://www.microsoft.com/technet/security/bulletin/ms05-014.mspx
http://www.microsoft.com/technet/security/bulletin/ms05-008.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely2
g. http://www.microsoft.com/technet/security/bulletin/MS04-040.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=48#widely2
h. http://www.microsoft.com/technet/security/bulletin/MS04-038.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely1
i. http://www.microsoft.com/technet/security/bulletin/MS04-025.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=30#widely1

Internet Explorer 0-day Vulnerabilities (at the time of disclosure)

http://www.sans.org/newsletters/risk/display.php?v=4&i=33#widely3
http://www.sans.org/newsletters/risk/display.php?v=4&i=29#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=26#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=27#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=51#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=51#widely4
http://www.sans.org/newsletters/risk/display.php?v=3&i=52#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=46#widely2
http://www.sans.org/newsletters/risk/display.php?v=3&i=45#widely4
http://www.sans.org/newsletters/risk/display.php?v=3&i=44#widely2
http://www.sans.org/newsletters/risk/display.php?v=3&i=43#widely2
http://www.sans.org/newsletters/risk/display.php?v=3&i=44#widely3
http://www.sans.org/newsletters/risk/display.php?v=3&i=42#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=43#widely2
http://www.sans.org/newsletters/risk/display.php?v=3&i=34#exploit1
http://www.sans.org/newsletters/risk/display.php?v=3&i=33#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely2

W3. Windows Libraries

W3.1 Description

Windows applications leverage a large number of system libraries often packaged in DLL files. These libraries are used for many common tasks such as HTML parsing, image format decoding, protocol decoding etc. 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 increases the number of systems available for attacks.

The critical libraries affected during past year:

a. Windows Graphics Rendering Engine Remote Code Execution (MS05-053)
b. Microsoft DirectShow Remote Code Execution (MS05-050)
c. Microsoft Color Management Module Remote Code Execution (MS05-036)
d. HTML Help Remote Code Execution (MS05-026, MS05-001, MS04-023)
e. Web View Remote Code Execution (MS05-024)
f. Windows Shell Remote Command Execution (MS05-049, MS05-016, MS04-037, MS04-024)
g. Windows Hyperlink Object Library Remote Code Execution (MS05-015)
h. PNG Image Processing Remote Code Execution (MS05-009)
i. Cursor and Icon Processing Remote Code Execution (MS05-002)
j. Windows Compressed Folder Remote Code Execution (MS04-034)
k. JPEG Processing Remote Code Execution(MS04-028)

For most of these vulnerabilities, exploit code is publicly available. Attacks exploiting these vulnerabilities have been seen in the wild. An example of a large-scale attack reported involved exploiting the **Cursor and Icon Handling** flaws to install malware on users' systems. Trojan Phel.A was reported to exploit the flaw in the HTML Help Library. Note that for some libraries such as HTML Help and Windows Shell, a newer update includes the older updates. Hence, only the latest update needs to be applied for yet unpatched systems.

W3.2 Operating Systems Affected

Windows NT 4, Windows 2000, Windows XP, Windows 2003

W3.3 CVE Entries

CVE-2003-1041, CVE-2004-0201, CVE-2004-0200, CVE-2004-0214, CVE-2004-0420, CVE-2004-0575, CVE-2004-0597, CVE-2004-1043, CVE-2004-1049, CVE-2004-1244, CVE-2005-0057, CVE-2005-0063, CVE-2005-1191, CVE-2005-1208, CVE-2005-1219, CVE-2005-2117, CVE-2005-2118, CVE-2005-2122, CVE-2005-2123, CVE-2005-2124, CVE-2005-2128

W3.4 How to Determine If You Are Vulnerable

These flaws can usually be best resolved by patching, since work-arounds are complicated due to multiple attack vectors. One can use Vulnerability Scanners to check if the appropriate update has been installed.

W3.5 How to Protect against Windows Libraries' Vulnerabilities

- Ensure that your Windows system has 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 both Windows 2000 and XP, or the Internet Connection Firewall in Windows XP systems to block inbound access to the affected ports. Using a properly configured personal/network firewall will also solve the problem.
- Due to a large number of attack vectors, Intrusion Prevention/Detection Systems as well as Anti-virus and Malware Detection Software are very helpful in protecting from these vulnerabilities.
- If you are running third-party applications on customized Windows 2000/XP platforms, please 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.

W3.6 References

Microsoft Graphics Rendering Engine Remote Code Execution
http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely1

Microsoft DirectShow Remote Code Execution
http://www.microsoft.com/technet/security/Bulletin/MS05-050.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=41#widely1

Microsoft Color Management Module Remote Code Execution
http://www.microsoft.com/technet/security/Bulletin/MS05-036.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=28#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=29#exploit1

HTML Help Remote Code Execution
http://www.microsoft.com/technet/security/bulletin/MS05-026.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely2
http://www.microsoft.com/technet/security/bulletin/MS05-001.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=2#widely1
http://www.microsoft.com/technet/security/bulletin/MS04-023.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely3

Web View Remote Code Execution
http://www.microsoft.com/technet/security/bulletin/MS05-024.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=19#widely2

Windows Shell Remote Command Execution
http://www.microsoft.com/technet/security/bulletin/MS05-016.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=15#widely6
http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely5
http://www.microsoft.com/technet/security/bulletin/MS04-024.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely5

Windows Hyperlink Object Library Remote Code Execution

http://www.microsoft.com/technet/security/bulletin/ms05-015.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely10

PNG Image Processing Remote Code Execution
http://www.microsoft.com/technet/security/bulletin/ms05-009.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely

Cursor and Icon Processing Remote Code Execution
http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=2#widely2
http://www.sans.org/newsletters/risk/display.php?v=3&i=51#widely2

Windows Compressed Folder Remote Code Execution
http://www.microsoft.com/technet/security/bulletin/MS04-034.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely3

JPEG Processing Remote Code Execution
http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx
http://www.sans.org/newsletters/risk/display.php?v=3&i=37#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=38#widely2

W4. Microsoft Office and Outlook Express

W4.1 Description

Microsoft Office is the most widely used email and productivity suite worldwide. The applications include Outlook, Word, Powerpoint, Excel, Visio, Frontpage, Access etc. Note that Outlook Express, a basic email client, is installed on all versions of Microsoft Windows starting with Windows 95. Vulnerabilities in these products can be exploited via 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 server such as News server that sends malicious responses to trigger a buffer overflow in email clients.

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

a. Cumulative Security Update for Outlook Express (MS05-030)
b. Microsoft OLE and COM Remote Code Execution (MS05-012)
c. Microsoft Office XP Remote Code Execution (MS05-005)

Exploit code and technical details are publicly available for all these vulnerabilities. A flaw in the Office Access component is yet unpatched and reportedly being exploited by a Trojan.

W4.2 Operating Systems Affected

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

W4.3 CVE Entries

CVE-2004-0848, CVE-2005-0044, CVE-2005-1213

W4.4 How to Determine If You Are at Risk

The Office and Outlook Express installations running without the patch referenced in the Microsoft Bulletins listed above are vulnerable. The simplest way is to use a Vulnerability Scanner.

W4.5 How to Protect against These 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
- Use Intrusion Prevention/Detection Systems and Anti-virus and Malware Detection Software to prevent malicious server responses and documents from reaching the end users.

W4.6 References

Microsoft Office XP Buffer Overflow
http://www.microsoft.com/technet/Security/bulletin/ms05-005.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely4

Microsoft OLE and COM Remote Code Execution
http://www.microsoft.com/technet/Security/bulletin/ms05-012.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely7

Cumulative Security Update for Outlook Express
http://www.microsoft.com/technet/security/bulletin/ms05-030.mspx
http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely4
http://www.sans.org/newsletters/risk/display.php?v=4&i=26#exploit3

Office Access Buffer Overflow (yet unpatched)
http://www.sans.org/newsletters/risk/display.php?v=4&i=15#exploit1
http://securityresponse.symantec.com/avcenter/venc/data/backdoor.ryejet.b.html

W5. Windows Configuration Weaknesses

W5.1 Description

The configuration weaknesses in Windows systems are still being exploited by newer families of bots and worms. These weaknesses typically fall under the following categories.

Weak passwords on Windows accounts or network shares

In the last couple of years the weak authentication scheme in Windows has made it to the "Top 10" windows vulnerabilities. LAN Manager (LM) hashes are known to be weak and are replaced by various versions of NTLM (NTLM AND NTLMv2) authentication. Although most current Windows environments have no need for LAN Manager (LM) support, Microsoft Windows locally stores legacy LM password hashes (also known as LANMAN hashes) by default on Windows NT, 2000 and XP systems (but not in Windows 2003).

Since LM uses a much weaker encryption scheme than more current Microsoft approaches (NTLM and NTLMv2), LM passwords can be broken in a relatively short period of time by a determined attacker. Even passwords that otherwise would be considered "strong" can be cracked by brute-force in under a week on current hardware. A hacker can either try known defaults, or check for common passwords or use a brute force attack also called a "dictionary" attack to guess the password of users' accounts. Tools like THC's Hydra can be used to remotely crack passwords. LophtCrack and John the Ripper are other well known password cracking or auditing programs.

Many families of worms or BOT Zombies like GaoBot, PhatBot and AgoBot spread through network shares that have weak passwords. These worms use a list of hardcoded passwords in an attempt to match the victim's password, enabling them to spread.

Default Configuration/Passwords for Servers

When installing Microsoft Data Engine (MSDE) or Microsoft SQL Server Desktop (MSDE2000), the default SQL Administrator account or "sa" account has a default blank password and uses SQL authetication. MSDE ships as a component of several applications such as Microsoft Office 2000 and other third party applications. This blank or Null password leaves it vulnerable to a worm. For instance, worms like Voyager Alpha Force, SQL Spida and Cblade use the above vulnerability.

IIS Servers by default have settings that make them vulnerable to attacks. Some accounts that are created by default at installation like IUSR_computername account have write access privileges even for anonymous users. Permissions on such accounts should be modified for restricted access.

IIS services such as FTP, NNTP or SMTP are enabled by default and are a ripe source of attacks. These IIS services should be disabled.

W5.2 Operating Systems Affected

Windows NT, Windows 2000, Windows XP and Windows 2003

W5.3 How to Protect against These Vulnerabilities

- Enforce strong password policy by accepting passwords that have a minimum number of characters (12 or higher if possible). Use tools like L0phtcrack or John The Ripper to audit accounts with weak passwords.
- Prevent Windows from storing the LM hash in Active Directory or SAM database by following the instructions posted by Microsoft.
- Tweak the registry to restrict Anonymous access to network shares.
- Modify default configuration settings on IIS servers and MS-SQL servers.

W5.4 References

GaoBot Information
http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html

Brute force scanning against MS SQL server accounts; Are you paranoid enough?
http://isc.sans.org/diary.php?date=2004-12-30

Unsecured SQL Server with Blank (NULL) SA Password Leaves Vulnerability to a Worm
http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q313418

CERT Vulnerability Note
http://www.kb.cert.org/vuls/id/635463

IIS 6.0 Security Best Practices
http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/596cdf5a-c852-4b79-b55a-708e5283ced5.mspx

How to use the RestrictAnonymous registry value in Windows 2000
http://support.microsoft.com/kb/q246261

Top Vulnerabilities in Cross-Platform Applications

C1. Backup Software

C1.1 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 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 and several malicious bots are using the published exploit code.

C1.2 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
- Symantec Veritas Storage Exec
- Computer Associates BrightStor ARCServe
- EMC Legato Networker
- Sun StorEdge Enterprise Backup Software (formerly Solstice Backup Software)
- Arkeia Network Backup Software
- BakBone Netvault Backup Software

C1.3 CVE Entries

CVE-2004-1172, CVE-2004-1389, CVE-2005-0260, CVE-2005-0349, CVE-2005-0357, CVE-2005-0358, CVE-2005-0491, CVE-2005-0496, CVE-2005-0581, CVE-2005-0582, CVE-2005-0583, CVE-2005-0771, CVE-2005-0772, CVE-2005-0773, CVE-2005-1009, CVE-2005-1019, CVE-2005-1018, CVE-2005-1272, CVE-2005-1547, CVE-2005-2051, CVE-2005-2079, CVE-2005-2080, CVE-2005-2535, CVE-2005-2611, CVE-2005-2715, CVE-2005-2996, CVE-2005-3116

C1.4 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
A listing of ports used by Veritas backup daemons is available here.

CA BrightStor ARCServe Backup Agent
TCP/6050, UDP/6051, TCP/6070, TCP/41523, UDP/41524

Sun and EMC Legato Networker
TCP/7937-9936

Arkeia Network Backup
TCP/617

BakBone Netvault Backup
TCP/20031 and UDP/20031

C1.5 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 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.

C1.6 References

Computer Associates Advisories

http://archives.neohapsis.com/archives/bugtraq/2005-08/0033.html
http://archives.neohapsis.com/archives/bugtraq/2005-04/0202.html
http://www.sans.org/newsletters/risk/display.php?v=4&i=31#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=15#other1
http://www.ca.com/at/local/partner/techtalk_mar05_faq.pdf (Ports Used by Backup Products)

Symantec Veritas Advisories

http://seer.support.veritas.com/docs/279553.htm
http://seer.support.veritas.com/docs/276604.htm
http://seer.support.veritas.com/docs/276605.htm
http://seer.support.veritas.com/docs/276606.htm
http://seer.support.veritas.com/docs/276533.htm
http://seer.support.veritas.com/docs/276607.htm
http://seer.support.veritas.com/docs/277567.htm
http://seer.support.veritas.com/docs/277566.htm
http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely4
http://www.sans.org/newsletters/risk/display.php?v=4&i=38#other3
http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely1
http://www.us-cert.gov/current/current_activity.html#VU378957

EMC Legato and Sun Advisories

http://www.legato.com/support/websupport/product_alerts/081605_NW_token_authentication.htm
http://www.legato.com/support/websupport/product_alerts/081605_NW_authentication.htm
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101886-1
http://www.sans.org/newsletters/risk/display.php?v=4&i=33#widely2

Arkeia Advisory

http://www.arkeia.com/securityfix/
http://www.sans.org/newsletters/risk/display.php?v=4&i=8#widely1

BakBone Advisory

http://www.sans.org/newsletters/risk/display.php?v=4&i=19#other1 (unpatched)
http://www.sans.org/newsletters/risk/display.php?v=4&i=14#other1

C2. Anti-virus Software

C2.1 Description

Anti-virus software is seen as a required basic tool within the "defense-in-depth" toolbox to protect systems today. Anti-virus software is now installed on almost all desktops, servers and gateways on various platforms to combat

virus outbreaks.

During the past year, there has been a shift in focus to exploit security products used by a large number of end users. This includes anti-virus and personal firewall software. The discovery of vulnerabilities in anti-virus software is not limited to just desktop and server platforms. Gateway solutions could also be affected. Compromising a gateway could potentially cause a much larger impact since the gateway is the outer layer of protection and the only protection for some threats in many small organizations.

Multiple buffer overflow vulnerabilities have been discovered in the anti-virus software provided by various vendors including Symantec, F-secure, Trend Micro, Mcafee, Computer Associates, ClamAV and Sophos. These vulnerabilities can be used to take a complete control of the user's system with limited or no user interaction.

Anti-virus software has also been found to be vulnerable to "evasion" attacks. By specially crafting a malicious file, for instance, an HTML file with an exe header, it may be possible to bypass anti-virus scanning. The evasion attacks can be exploited to increase the virus infection rate.

C2.2 Operating Systems Affected

Any system installed with anti-virus software or virus scan engine meant to scan malicious code could be affected. This includes solutions installed on desktops, servers and gateways. Any platform could be affected including all Microsoft Windows and Unix systems.

C2.3 CVE Entries

AhnLab
CVE-2005-3029, CVE-2005-3030
Avast!
CVE-2005-2384, CVE-2005-2385
AVIRA
CVE-2005-2957
BitDefender
CVE-2005-3154
ClamAV
CVE-2005-2450, CVE-2005-2920
Computer Associates
CVE-2005-1693
HAURI
CVE-2004-2720, CVE-2005-2670, CVE-2005-2041
F-Secure
CVE-2004-2405, CVE-2005-2937, CVE-2005-0350
Kaspersky
CVE-2005-2937, CVE-2005-3142
Mcafee
CVE-2005-0643, CVE-2005-0644
Sophos
CVE-2005-2768
Symantec
CVE-2005-0249
Trend Micro
CVE-2005-0533
ZoneAlarm
CVE-2005-1693

C2.4 How to Determine If You Are Vulnerable

If you are running any release of any anti-virus software that has not been updated to the latest version, you are likely to be affected.

C2.5 How to Protect against Anti-virus Software Vulnerabilities

- Ensure that all of your antivirus software is regularly and automatically updated.
- Regularly check your vendor website for upgrades, patches and security advisories. A list of anti-virus vendors is provided in the References below. Note that the list may not be exhaustive.
- If you have deployed anti-virus software on gateway and desktops, it is recommended to use different anti-virus vendor solutions for gateway and desktop. In the event one is vulnerable, it will not result in a single point of failure.

C2.6 References

Below is a list of anti-virus vendors to check for upgrades, patches and security advisories.

Anti-virus Security Advisories

http://www.sans.org/newsletters/risk/display.php?v=4&i=6 (Symantec)
http://www.sans.org/newsletters/risk/display.php?v=4&i=6 (F-Secure)
http://www.sans.org/newsletters/risk/display.php?v=4&i=8#widely2 (Trend Micro)
http://www.sans.org/newsletters/risk/display.php?v=4&i=12#widely1 (McAfee)
http://www.sans.org/newsletters/risk/display.php?v=4&i=21#widely1 (Computer Associates)
http://www.sans.org/newsletters/risk/display.php?v=4&i=30#widely1 (ClamAV)
http://www.sans.org/newsletters/risk/display.php?v=4&i=38 (ClamAV)
http://www.sans.org/newsletters/risk/display.php?v=4&i=34#other2 (HAURI)
http://www.sans.org/newsletters/risk/display.php?v=4&i=35#widely2 (Sophos)
http://www.sans.org/newsletters/risk/display.php?v=4&i=38#other2 (AhnLab and AVIRA)
http://www.sans.org/newsletters/risk/display.php?v=4&i=42#other4 (AhnLab)
http://www.sans.org/newsletters/risk/display.php?v=4&i=40#other3 (Kaspersky)

Anti-virus Evasion Issues

http://www.kb.cert.org/vuls/id/968818
http://www.uniras.gov.uk/vuls/2004/380375/mime.htm
http://www.sans.org/newsletters/risk/display.php?v=4&i=43#other4

Other Anti-virus Resources

http://www.cert.org/other_sources/viruses.html
http://www.virusbtn.com/
http://www.eicar.com/
http://www.wildlist.org/

C3. PHP-based Applications

C3.1 Description

PHP is the most widely used scripting language for the web. According to some reports, 50% of the Apache servers world-wide have PHP installed. A large number of Content Management Systems (CMS), portals, Bulletin Boards, Discussion Forums are written in PHP. There has not been a single week during the last year that a problem was not reported in some software using PHP. The typical vulnerabilities that have been exploited during the past year are:

a. Vulnerabilities in the PHP package itself. Exploit code is available for some of these vulnerabilities.
b. Remote File include vulnerabilities in the applications using PHP. These are very common and easy to exploit. These flaws allow an attacker to run code of his choice on the vulnerable web server.
c. Remote Command Execution vulnerabilities in the applications using PHP. These are easy to exploit and the discoverers typically post a proof of concept code on the Internet. Santy worm resulted from such a vulnerability in the popularly used bulletin board- phpBB.
d. SQL Injection vulnerabilities in the applications using PHP. These are easy to exploit and are actively used to recover password hashes for administrators of the PHP applications.
e. Remote Code Execution vulnerabilities in libraries implemented using PHP. For instance, PHP XML-RPC and Pear XML-RPC libraries are used by a number of software projects. Lupper worm is exploiting remote code execution vulnerabilities in these libraries.

The last three types of vulnerabilities result from lack of sanitization of user-supplied input. The availability of web scanning tools has automated the process of finding these vulnerabilities.

C3.2 Affected Software

Web servers that are not running the latest version of PHP package. If you are running other PHP software that is not at its latest version, the web server is most likely vulnerable.

C3.3 CVE Entries

CVE-2004-0594, CVE-2005-3389, CVE-2005-3390

Note: These do not include the large number of CVE entries associated with a PHP-based applications.

C3.4 How to Determine If You Are at Risk

Scanning the web servers periodically with Vulnerability Scanners is your best bet since the number of vulnerabilities in PHP applications reported every week can be difficult to keep track of, and especially if you are running a large number of PHP-based applications on your servers.

C3.5 How to Protect against PHP Vulnerabilities

- Apply all vendor patches for PHP and PHP-based applications.
- Frequent web scanning is recommended in environments where a large number of PHP applications are in use.
- Use the following PHP Configuration that is safer:
  - register_globals (should be off)
  - allow_url_fopen (should be off)
  - magic_gpc_quotes (should be off for well written software, should be on for poorly written PHP 3 and PHP 4 scripts,)
  - safe_mode and open_basedir (should be enabled and correctly configured)
- Configure Apache mod_security and mod_rewrite filters to block PHP attacks.
- Use tools like Paros Proxy for conducting automated SQL Injection tests against your PHP applications.
- Upgrade to PHP 5 as it will eliminate many latent PHP security issues.
- Follow the "Least Privilege" principle for running PHP using tools like PHPsuExec, php_suexec orsuPHP from suPHP.
- Use any Intrusion Prevention/Detection Systems to block/alert on malicious HTTP requests.

C3.6 References:

PHP Vulnerabilities

http://www.hardened-php.net/advisory_202005.79.html
http://www.hardened-php.net/advisory_152005.67.html
http://www.hardened-php.net/advisory_142005.66.html
http://www.sans.org/newsletters/risk/display.php?v=3&i=50#widely4
http://www.sans.org/newsletters/risk/display.php?v=3&i=23#other1
http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely4
http://www.sans.org/newsletters/risk/display.php?v=3&i=48#exploit1

Hardened PHP Project

http://www.hardened-php.net

OWASP Webpage (Contains tools and documents for testing Web Application Vulnerabilities)

http://www.owasp.org

PHP Security Features

http://au.php.net/features.safe-mode

C4. Database Software

C4.1 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, the databases are often a target of attack. Since databases are extremely complex applications and are normally a collection of a number of programs, this results in a large number of attack vectors. The most common vulnerabilities in most database systems found today can be classified into:

- Buffer overflows in processes that listen on well known TCP/UDP ports
- SQL Injection via the web front end of the database
- Databases running in default configuration with default usernames and passwords
- Databases running with 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 (proprietary, runs on multiple 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. For example, Microsoft SQL server can be accessed via TCP port 1433, Oracle via TCP port 1521, IBM DB2 via ports 523 and 50000 up, MySQL via TCP port 3306, and PostgreSQL via TCP port 5432.

During the past year, Oracle has issued cumulative updates that patch hundreds of vulnerabilities. Hence, even if all the vulnerabilities corrected via a cumulative patch are not of critical nature, the administrators are forced to apply the patches to correct a few critical issues.

Proof of concept exploits for many database flaws are readily available on the Internet.

C4.2 Operating Systems Affected

The open source databases are available on virtually every operating system in common use today. Most commercial DBMS also run on multiple platforms

C4.3 CVE Entries

These are the entries released since July 2004. Earlier vulnerabilities can be found in previous editions of the Top 20.

Oracle
CVE-2004-0637, CVE-2004-0638, CVE-2004-1338, CVE-2004-1363, CVE-2004-1364, CVE-2004-1365, CVE-2004-1366, CVE-2004-1369, CVE-2004-1370, CVE-2004-1371, CVE-2005-1495, CVE-2004-1774
Note: All CVEs from Oracle Cumulative Patch Updates have not been listed here.

MySQL
CVE-2004-0627, CVE-2004-0628, CVE-2004-0836, CVE-2005-0684, CVE-2005-1274, CVE-2005-2558
PostgreSQL
CVE-2005-0244, CVE-2005-0247
IBM DB2
CVE-2004-0795, CVE-2004-1372

C4.4 How to Determine If You Are Vulnerable

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. It is not sufficient to check a simple list of the applications that have been installed! 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 any vulnerability scanners or tools from database vendors such as MySQL Network Scanner, Microsoft SQL server tool.

C4.5 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://otn.oracle.com/deploy/security/alerts.htm)
  - MySQL (http://lists.mysql.com/)
  - PostgreSQL (http://www.postgresql.org/community/)
  - Microsoft SQL (http://www.microsoft.com/technet/security/bulletin/notify.mspx)
  - IBM DB2 (http://www-306.ibm.com/software/data/db2/udb/support/)
- Ensure that the DBMS and applications have been secured:
  - Use minimal privileges.
  - Remove/change default passwords on the database's privileged and system accounts before deploying the system on the network.
  - Use stored procedures where possible.
  - Remove/disable unnecessary stored procedures.
  - Set length limits on any form fields.
  - There are several useful resources to help secure DBMS mentioned in the references section.
- 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)

C4.6 References

SANS Reading Room on Database Security
http://www.sans.org/rr/catindex.php?cat_id=3

Oracle
SANS Comprehensive Security Checklist for Oracle
http://www.sans.org/score/oraclechecklist.php
https://store.sans.org/store_item.php?item=80

CIS Oracle Benchmark Tool
http://www.cisecurity.org/bench_oracle.html

Oracle security information can be found at

http://www.petefinnigan.com/orasec.htm
http://otn.oracle.com/deploy/security/index.html

MySQL
SecurityFocus step-by-step guide to securing MySQL
http://www.securityfocus.com/infocus/1726

MySQL Security
http://dev.mysql.com/doc/mysql/en/Security.html

PostgreSQL Security Guide
http://www.postgresql.org/docs/7/interactive/security.html

Microsoft SQL Security Guide
http://www.microsoft.com/sql/techinfo/administration/2000/security/default.mspx

IBM DB2
http://www.net-security.org/dl/articles/Securing_IBM_DB2.pdf

C5. File Sharing Applications

C5.1 Description

Peer to Peer File Sharing Programs (P2P) are used by a rapidly growing user base. These applications are used to download and distribute data such as music, video, graphics, text, source code etc. P2P applications are also used legitimately for distribution of OpenSource/GPL binaries and ISO images of bootable Linux distributions. However, often times the data is either of a questionable nature or is copyrighted.

P2P programs 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.

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.

The main threats arising from P2P software are:

- Remotely exploitable vulnerabilities in P2P applications that can be used to compromise P2P clients or servers.
- Viruses and bots use P2P shared folders for spreading by copying malicious files into these folders with enticing filenames.
- P2P software is generally bundled with spyware and adware software. This increases the spyware/adware infection in an organization.
- Attackers can masquerade malicious files as legitimate music or video files. When the users download these files, their system can be infected and used as a "bot".
- P2P shares typically have no passwords or weak passwords, a flaw that can be exploited to infect the share with malicious files.
- An organization can be liable to lawsuits for copyright infringement.
- P2P traffic can contribute substantially to overall bandwidth and make other mission-critical applications slower. This can be especially threatening to quality of service for voice and video traffic in an organization.

Exploit code is available for some of the buffer overflow vulnerabilities in the P2P software. According to Symantec's research, in the second half of 2004, 6% of internet attacks tried to exploit vulnerabilities in eDonkey and another 5% in Gnutella.

The number of threats using P2P, IM, IRC, and CIFS within Symantec's top 50 malicious code reports has increased by 39% over the previous six-month period.

C5.2 Operating Systems Affected

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

C5.3 CVE Entries

CVE-2004-1114, CVE-2004-1286, CVE-2004-1892, CVE-2004-2433, CVE-2005-0595, CVE-2005-1806

C5.4 How to Determine If You Are Vulnerable

Detecting P2P activity on the network can prove to be challenging.

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

C5.5 How to Protect against P2P Software Vulnerabilities

- Regular users should not be permitted to install software, especially peer to peer applications. To prevent regular users from installation of unauthorized software, it is recommended to deny Administrative level privileges for regular users. To prevent accidental installation of unauthorized software by Administrator level users, tools like Microsoft DropMyRights can be used for securing of any 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.
- Egress filtering should restrict access to any ports not required for business purposes, although as more P2P applications move to http, this will prove less effective.
- Monitor your network for P2P traffic and address violations of policy through appropriate channels. That can be achieved by monitoring of firewall, IDS logs. Enterprise solutions are available for detection and blocking of unauthorized P2P and IM connections.
- On individual workstation tools like Microsoft PortQry and Port Reporter can be used to monitor and log unusual network activity.
- Use enterprise-wide anti-virus and antispyware 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. 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 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 (there are commercial and open source versions of the product) can be used to detect changes in files.

Common protocols and ports used by peer-to-peer applications

P2P Service	Default/primary port or port range, TCP	Default/primary port or port range, UDP
BearShare	6346	
Bittorrent	2181, 6881-6999	
Blubster		41170-41350
eDonkey	4661-4662	5737
eDonkey2000	4661-4662	4665
eMule	4661-4662,4711	4665,4672
Gnutella	6346/6347	6346/6347
Grouper	8038	8038
Kazaa	1214	1214
Limewire	6346/6347	6346/6347
Morpheus	6346/6347	6346/6347
Shareaza	6346	6346

WinMx	6699	6257

C5.6 References

US DHS Information Bulletin "Unauthorized Peer-to-Peer (P2P) Programs on Government Computers"
http://www.dhs.gov/interweb/assetlibrary/IAIP_UnauthorizedP2PProgramsGovtComp_041905.pdf
Federal Law Enforcement Announces Operation D-Elite, Crackdown on P2P Piracy Network: First Criminal Enforcement Against BitTorrent Network Users
http://www.usdoj.gov/criminal/cybercrime/BitTorrent.htm
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
http://www.ftc.gov/bcp/workshops/filesharing/presentations/hale.pdf
Symantec Internet Security Threat Report - Trends for July 04- December 04
Volume VII, Published March 2005
http://ses.symantec.com/pdf/ThreatReportVII.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
Identifying P2P users using traffic analysis - Yiming Gong - 2005-07-21
http://www.securityfocus.com/infocus/1843
Sinit P2P Trojan Analysis
http://www.lurhq.com/sinit.html
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
Peer-to-Peer (P2P) Security and QoS Frequently Asked Questions (CheckPoint)
http://secureknowledge.checkpoint.com/pub/sk/docs/public/firewall1/ng/pdf/p2p_faq.pdf

C6. DNS Software

C6.1 Description

The Domain Name System (DNS) is a critical Internet mechanism that primarily facilitates the conversion of globally unique host names into a corresponding globally unique Internet Protocol address 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, DNS cache poisoning vulnerabilities were exploited to redirect users to malicious domains to install malware on users' systems. Open recursive DNS servers are actively being used as DDoS reflectors providing a huge amplification factor.

C6.2 Affected Software

- Symantec Gateway Security
- Symantec Enterprise Firewall
- Symantec VelociRaptor
- DNSmasq DNS Server
- Windows NT and Windows 2000 (prior to SP3) DNS servers in the default configuration
- Windows DNS server forwarding requests to a BIND DNS server running version 4.x or 8.x
- Windows DNS server forwarding requests to another vulnerable Windows DNS server

C6.3 CVE Entries

CVE-2005-0817, CVE-2005-0877

C6.4 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.

C6.5 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 generally 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 CERT's UNIX Security Checklist.
- Apply appropriate firewall rules for any DNS servers inside a network that are not required to be accessible from the Internet.
- To secure the zone transfers between a primary and a secondary DNS server in a cryptographic way, configure the servers to use the DNS Transaction Signatures (TSIG).
- Jail: 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.
- Do not allow your recursive DNS servers to be used except by your own network blocks unless required. Firewalls or DNS configurations files can prevent this scenario 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.
- Do not allow your recursive DNS servers to be used except by your own network blocks unless required. Firewalls or DNS configurations files can prevent this scenario in most cases.

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.mspx
http://www.dns.net/dnsrd/

DNSSEC Deployment

http://www.dnssec-deployment.org/
http://www.dnssec.net
http://csrc.nist.gov/publications/drafts/DRAFT-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://www.isc.org/index.pl?/sw/bind/bind-security.php

C7. Media Players

C7.1 Description

Media players are popularly used and have an install base of millions of systems. The increase in broadband connections has facilitated more content being 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.

A number of vulnerabilities have been discovered in various media players during 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

C7.2 Operating Systems Affected

Microsoft Windows, Unix/Linux and Apple Mac OS X

C7.3 CVE Entries

RealPlayer and Helix Player
CVE-2004-0550, CVE-2004-1094, CVE-2004-1481, CVE-2005-0189, CVE-2005-0191, CVE-2005-0455, CVE-2005-0611, CVE-2005-0755, CVE-2005-1766, CVE-2005-2052, CVE-2005-2054, CVE-2005-2055, CVE-2005-2710, CVE-2005-2055
iTunes
CVE-2005-0043, CVE-2005-1248
Winamp
CVE-2004-0820, CVE-2004-1119, CVE-2004-1150, CVE-2004-1896, CVE-2005-2310
Quicktime
CVE-2004-0431, CVE-2004-0926, CVE-2005-2743, CVE-2005-2753, CVE-2005-2754
Windows Media Player
CVE-2004-1244, CVE-2004-1324
Macromedia Flash Player
CVE-2005-2628

C7.4 How to Determine If You Are at Risk

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.

C7.5 How to Protect against These 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.

C7.6 References

RealNetworks
Media Player Products Home Page

http://www.realnetworks.com/products/media_players.html

Security Reports
http://service.real.com/help/faq/security/
http://service.real.com/help/faq/security/051110_player/EN/
http://www.sans.org/newsletters/risk/display.php?v=4&i=40#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=16#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=10#exploit1
http://www.sans.org/newsletters/risk/display.php?v=4&i=9#widely2
http://www.sans.org/newsletters/risk/display.php?v=3&i=43#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=39#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=23#widely4

Helix Player
Home Page
https://player.helixcommunity.org/

News, Including Security Announcements
https://helixcommunity.org/news/

Apple
QuickTime Home Page
http://www.apple.com/quicktime/

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=4&i=45#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=19#widely3
http://www.sans.org/newsletters/risk/display.php?v=4&i=2#widely3
http://www.sans.org/newsletters/risk/display.php?v=4&i=3#exploit1

Nullsoft Winamp
Home Page
http://www.winamp.com/
http://www.winamp.com/about/news.php

Security Reports
http://www.sans.org/newsletters/risk/display.php?v=4&i=5#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=47#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=36#widely1
http://www.sans.org/newsletters/risk/display.php?v=3&i=34#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=3&i=51#04.51.1
http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely5

Macromedia Flash Player

Homepage
http://www.macromedia.com/software/flashplayer

Security Reports
http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely3

C8. Instant Messaging Applications

C8.1 Description

Instant Messaging (IM) applications are being used today by millions of users both for personal and business purposes. IM applications are available for virtually all platforms including the handheld devices. Today's most popular IM applications are:

Yahoo! Messenger, AOL Instant Messenger, MSN Messenger, Jabber, Trillian, Skype and IRC. GoogleTalk has just been released and is also gaining ground. A web version of many of these applications is also available whereby a user does not need to install the IM client on his system. These applications provide an increasing security threat to an organization. The major threats are the following:

a. Vulnerabilities in IM applications that could be used to compromise a user's system. During last year buffer overflows were discovered in the AIM URI handler as well as MSN Messenger PNG Image Processing. Exploit code is available for these vulnerabilities.
b. Most of these applications have the capability of transferring files. This feature is being currently exploited by many IM worms to infect users' systems with malware.
c. The file transfers can also result in leaking sensitive information.
d. Many worms and bots use IRC channels to communicate with the attacker. The IRC channels can also be used for launching DDoS attacks.
e. Some of these applications can carry voice data, which in addition to file transfers, may result in rogue bandwidth utilization.

C8.2 Operating Systems Affected

Instant Messaging Applications are available for all platforms including Windows, UNIX and Mac OS.

C8.3 CVE Entries

CVE-2004-0597, CVE-2004-0636, CVE-2005-0243, CVE-2005-0562, CVE-2005-3265, CVE-2005-3267

C8.4 How to Protect against IM Vulnerabilities

- Establish corporate policy outlining "appropriate" IM usage within the company. Run routine audits of Firewall and Proxy logs to enforce IM usage policy.
- Restrict the end users' ability to install software on the client workstation. Can be done by revoking workstation admin rights.
- Ensure that any installed messenger software such as Yahoo, MSN, AOL, Trillian etc is up to date with all vendor patches.
- Configure any Intrusion Prevention/Detection Systems to alert on any file transfers that use any of the messaging programs.
- If the site security policy permits:
    - Block the following ports at the firewall. Note that this does not offer a complete protection since some of these applications can bypass firewall rules.
        - 1503/tcp: MSN Messenger Application Sharing
        - 1863/tcp: Microsoft .NET Messenger, MSN Messenger
        - 4443/tcp: Yahoo Messenger File Sharing
        - 5050/tcp: Yahoo Messenger
        - 6891/tcp: MSN Messenger File Transfers
        - 5190-5193/tcp: AOL Instant Messenger
        - 13324-13325/tcp: MSN Messenger Audio and Video Conferencing
        - 5222-5223/tcp: Google Talk
        - 4000/udp - ICQ
    - Block access to webpages containing links with URLs such as "aim:" or "ymsgr:". This can prevent exploitation of the flaws in the URI handlers. Another option is to carefully remove just these registry keys in the "HKEY_CLASSES_ROOT".
    - For AOL block the following destination: oscar.login.aol.com
    - For Google Talk, block the following destination: talk.google.com
    - Yahoo Instant Messenger will tunnel its traffic over a variety of ports, including finger, discard, chargen and smtp. To be effective, block the following destination in addition to its ports above: cs.yahoo.com &

scsa.yahoo.com
    - Use software restriction policies or other mechanisms to prevent execution of the instant messenger clients such as msmsgs.exe, aim.exe, ypager.exe, icq.exe, trillian.exe.
- Filter all HTTP traffic through an authenticating proxy server. A proxy server will give you additional abilities to filter IM traffic.

C8.5 References

Threats to Instant Messaging
http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf
http://www.eweek.com/article2/0,1895,1864869,00.asp

IM Buffer Overflows
http://www.sans.org/newsletters/risk/display.php?v=3&i=32#widely1 (AOL)
http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely5 (Windows and MSN Messenger)
http://www.sans.org/newsletters/risk/display.php?v=4&i=15#widely7 (MSN Messenger)
http://www.sans.org/newsletters/risk/display.php?v=4&i=43#other1 (Skype)

C9. Mozilla and Firefox Browsers

C9.1 Description

Mozilla Firefox version 1.0 was officially released in November 2004. Mozilla and Firefox have emerged as viable alternatives to Internet Explorer and have been steadily gaining the browser market share. With this increased usage, the browsers have come under greater scrutiny by security auditors and hackers alike, resulting in multiple vulnerabilities discovered during last year. Many of the flaws discovered are critical in nature and allow a malicious webpage to completely compromise a client system. Exploit code for leveraging these vulnerabilities is publicly available as well.

C9.2 Operating Systems Affected

Mozilla and Firefox browsers on Windows and Linux systems

C9.3 CVE Entries

CVE-2005-2270, CVE-2005-0592, CVE-2005-0593, CVE-2005-0752, CVE-2005-1155, CVE-2005-1156, CVE-2005-1157, CVE-2005-1158, CVE-2005-1160, CVE-2005-1476, CVE-2005-1477, CVE-2005-1531, CVE-2005-1937, CVE-2005-2262, CVE-2005-2267, CVE-2005-2270, CVE-2005-2268, CVE-2005-2269, CVE-2005-2270, CVE-2005-2602, CVE-2005-2706, CVE-2005-2701, CVE-2005-2705, CVE-2005-2706, CVE-2005-2707, CVE-2005-2871, CVE-2005-2968

C9.4 How to Determine If You Are at Risk and Protect against These Vulnerabilities

- If you are running Firefox or Mozilla without the latest version, you are at risk. Firefox now has both an automated and manual tool that you can use to check for updates. However, you should visit the Firefox site regularly to ensure timely application of patches.
- Use any Vulnerability Scanner to detect vulnerable installations.
- Use Intrusion Prevention/Detection Systems and Anti-virus and Malware Detection Software to block malicious HTML script code.

C9.5 References

Mozilla Firefox Vulnerabilities
http://www.sans.org/newsletters/risk/display.php?v=4&i=39#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=38#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=37#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=38#exploit1
http://www.sans.org/newsletters/risk/display.php?v=4&i=28#widely8
http://www.sans.org/newsletters/risk/display.php?v=3&i=37#widely2

C10. Other Cross-platform Applications

C10.1 Description

This section of the Top-20 lists vulnerabilities in widely deployed products that cannot be classified into the other categories. In most cases, these vulnerabilities can be exploited for remote code execution. Some of the vulnerabilities may even allow an enterprise-wide compromise. Exploit code is available on the Internet and large-scale scanning for the vulnerable systems has been observed.

a. Computer Associates License Manager Overflows (CVE-2005-0581, CVE-2005-0582, CVE-2005-0583)

b. Novell eDirectory iMonitor and ZENWorks Buffer Overflows (CVE-2005-2551, CVE-2005-1543)
c. Computer Associates Message Queuing Vulnerabilities (CVE-2005-2668)
d. Sun Java Security Vulnerabilities (CVE-2004-1029, CVE-2005-0418, CVE-2005-0836, CVE-2005-1973, CVE-2005-1974)
e. HP Radia Management Software Overflows (CVE-2005-1825, CVE-2005-1826)
f. Snort BackOrifice Preprocessor Buffer Overflow (CVE-2005-3252)
g. RSA SecurID Web Agent Overflow (CVE-2005-1471)

C10.2 CVE Entries

CVE-2005-0581, CVE-2005-0582, CVE-2005-0583, CVE-2005-2551, CVE-2005-1543, CVE-2005-2668, CVE-2004-1029, CVE-2005-0418, CVE-2005-0836, CVE-2005-1973, CVE-2005-1974, CVE-2005-1825, CVE-2005-1826, CVE-2005-3252, CVE-2005-1471

C10.3 How to Determine If You Are at Risk and Protect against These Vulnerabilities

If you are running these products against the latest patches, you are vulnerable. Apply the patches from the vendors for these vulnerabilities. Work-arounds are listed in the SANS @RISK newsletter.

C10.4 References

CA License Manager Overflows
http://supportconnectw.ca.com/public/reglic/downloads/licensepatch.asp#alp
http://supportconnectw.ca.com/public/ca_common_docs/security_notice.asp
http://www.sans.org/newsletters/risk/display.php?v=4&i=9#widely1

Novell eDirectory iMonitor and ZENWorks Overflow
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098568.htm
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2972038.htm
http://www.sans.org/newsletters/risk/display.php?v=4&i=33#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=20#widely1

Computer Associates Message Queuing Vulnerabilities
http://archives.neohapsis.com/archives/bugtraq/2005-08/0292.html
http://www.sans.org/newsletters/risk/display.php?v=4&i=34#widely1
http://www.sans.org/newsletters/risk/display.php?v=4&i=42#exploit2

Sun Java Security Vulnerabilities
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57591-1
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57740-1
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101748-1
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101749-1
http://www.sans.org/newsletters/risk/display.php?v=3&i=47#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=12#widely2
http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely10

HP Radia Management Software Overflows
http://archives.neohapsis.com/archives/bugtraq/2005-06/0009.html
http://www.sans.org/newsletters/risk/display.php?v=4&i=22#other1
http://www.sans.org/newsletters/risk/display.php?v=4&i=18#other2
http://www.sans.org/newsletters/risk/display.php?v=4&i=30#exploit1

Snort BackOrifice Preprocessor Overflow
http://www.snort.org/pub-bin/snortnews.cgi#99
http://www.sans.org/newsletters/risk/display.php?v=4&i=42#widely1

RSA SecuID Web Agent Overflow
http://www.kb.cert.org/vuls/id/790533
http://www.sans.org/newsletters/risk/display.php?v=4&i=42#widely1

Top Vulnerabilities in UNIX Systems

U1. UNIX Configuration Weaknesses

U1.1 Description

Most of the Unix/Linux systems include in their default installation a number of standard services. Over the years, security savvy administrators have either been turning the non-required services off or firewalling them from the Internet. The reference section points to detailed write-ups about secure UNIX configurations in general.

Of particular interest this year are attacks against SSH. SSH is an interactive service that is available on most UNIX systems. Since the service encrypts data when it traverses the network, if the SSH version is fully patched, the service is generally assumed to be safe. However, this was one of the services very popularly targeted during the past year using brute-force password-guessing attacks. Systems with weak SSH passwords for typical user accounts were actively compromised; privilege escalations were then used to gain root access, and install root-kits to hide the compromise. It is important to know that brute forcing passwords can be another technique to compromise even a fully patched system. It is recommended to use public key authentication mechanism offered by most SSH implementations like OpenSSH to thwart such attacks. These attacks can be extended to other interactive services like telnet, ftp etc.

U1.2 Affected Versions

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

U1.3 How to Protect against These Vulnerabilities

- Don't use default passwords on any accounts.
- Don't use weak passwords or passwords based on dictionary words. Audit your machines to ensure your password policy is being adhered to. Install the latest vendor patches regularly to mitigate vulnerabilities in exposed services. Patch management is a critical part of the risk management process.
- Limit the number of login attempts to exposed services.
- Limit the accounts that can log in over the network; root should not be one of them. Consider employing firewall rules to limit where any remote logins, such as SSH, can occur from.
- 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 usage of PAM authentication modules, implement PAM modules that check for password's strength.
- Firewall services that do not require access to the Internet.
- Use The Center for Internet Security benchmarks from 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.
- Consider moving services from their default port where possible.

U1.4 References

SSH Brute Force Attacks and Counter Measures

http://isc.sans.org/diary.php?date=2004-11-04
http://isc.sans.org/diary.php?date=2004-11-02
http://isc.sans.org/diary.php?date=2004-09-11
http://isc.sans.org/diary.php?date=2004-08-30
http://isc.sans.org/diary.php?date=2004-08-29
http://isc.sans.org/diary.php?date=2004-08-22
http://seclists.org/lists/firewall-wizards/2005/Jun/0154.html
http://www.counterpane.com/alert-cis20040910-1.html
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1094140,00.html
http://www.frsirt.com/exploits/08202004.brutessh2.c.php

General UNIX Security Resources

http://www.cisecurity.org
http://www.bastille-linux.org

U2. Mac OS X

U2.1. Description

The Mac OS X was released by Apple in 2001 as a solid UNIX-based Operating System. Although Mac OS X has security features implemented out of the box such as built-in personal firewall, un-necessary services turned off by default and easy ways to increase the OS security, the user still faces many vulnerabilities.

Mac OS X also includes the Safari web browser. Multiple vulnerabilities have been found in this browser and in certain cases exploit code has also been posted publicly.

Apple frequently issues Mac OS X cumulative security updates that tend to include fixes for a large number of vulnerabilities with risk ratings ranging from critical to low. This complicates the tracking of vulnerabilities for this OS, and the best way to ensure security is to apply the latest cumulative patch

U2.2. How to determine If You Are Vulnerable

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. If you do not see any important packages patches available, you may be safe:

a. Choose System Preferences from the Apple Menu.
b. Choose Software Update from the View menu.
c. Click Update Now.
d. Check the items available

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

U2.3. CVE Entries

CVE-2005-0126, CVE-2005-0418, CVE-2005-0970, CVE-2005-1331, CVE-2005-1337, CVE-2005-1342, CVE-2005-1721, CVE-2005-2501, CVE-2005-2502, CVE-2005-2507, CVE-2005-2518

Safari: CVE-2005-1474, CVE-2005-2516, CVE-2005-2517, CVE-2005-2522

U2.4. How to Protect against Mac OS X 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/macosx/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 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.

U2.5 References

Mac OS X Vulnerabilities
http://www.sans.org/newsletters/risk/display.php?v=4&i=23#widely3
Apple Product Security
http://www.apple.com/support/security/
SecureMac
http://www.securemac.com/
Macintosh Security
http://www.macintoshsecurity.com/
Security Announce
http://lists.apple.com/mailman/listinfo/security-announce
CISecurity MAC OS X Benchmark
http://www.cisecurity.org/bench_osx.html
Securing Mac OS X 10.4 Tiger
http://www.corsaire.com/white-papers/050819-securing-mac-os-x-tiger.pdf
Securing Mac OS X 10.3 Panther
http://www.corsaire.com/white-papers/040622-securing-mac-os-x.pdf

Top Vulnerabilities in Networking Products

N1. Cisco IOS and non-IOS Products

N1.1 Description

Cisco's Internetwork Operating System (IOS) is Cisco's standard router and switch operating system. While not all of Cisco's routers and switches run IOS, there is an effort to transition them to IOS at the earliest possible opportunity. IOS is by far the most common enterprise router and switch operating system in the world, powering nearly 85% of the global Internet backbone. IOS has often enjoyed a reputation for security and robustness. It has long been believed that, as embedded devices, Cisco routers and switches were immune to severe security vulnerabilities. However, serious security research over the past year has revealed several vulnerabilities that can result in denial-of-service conditions or remote code execution vulnerabilities.

The critical vulnerabilities that appeared in Cisco IOS within the past year are:

a. Remote Denial-of-Service in BGP Processing (CVE-2004-0589)
b. Remote Denial-of-Service in SNMP Processing (CVE-2004-0714)
c. Remote Denial-of-Service in OSPF Processing (CVE-2004-1454)
d. Remote Code Execution in IPv6 Processing (CVE-2005-2451)
e. Remote Code Execution in Firewall Authentication Proxy (CVE-2005-2841)

While most of Cisco's network hardware runs Cisco's Internetwork Operating System, some lines of hardware run different, more application-specific operating systems. Primary examples include the CatOS-based Catalyst line of switches, the PIX firewall, and the Cisco CallManager systems. While these systems form a minority of Cisco's product line, they still have very high penetration into the enterprise switching, firewall, and voice markets.

The critical vulnerabilities that appeared in non-IOS-based Cisco products within the past year are:

f. Remote Code Execution in Cisco CallManager (CVE-2005-2244)
g. Hardcoded Username and Password in Cisco Wireless LAN Solution Engine (CVE-2004-0391)
h. Hardcoded SNMP Community Strings in Cisco IP/VC (CVE-2005-0612)
i. Remote Code Execution in Cisco Collaboration Server (CVE-2004-0650)

The critical vulnerabilities that appeared in IOS as well as non-IOS-based Cisco products within the past year are:

j. Cisco Devices IPSec Handling Vulnerabilities - PROTOS IPSec Test Suite

Exploit code is available for some of these flaws.

N1.2 Versions Affected

- Cisco IOS versions 11.1 through 12.4 are vulnerable to at least one of the above vulnerabilities (a) through (e) and (j).
- Cisco CallManager (CCM) 3.2 and earlier, 3.3 before 3.3(5), 4.0 before 4.0(2a)SR2b, and 4.1 4.1 before 4.1(3)SR1 are vulnerable to (f).
- Cisco wireless LAN Solution Engine versions 2.0 through 2.5 are vulnerable to (g).
- Cisco IP/VC Videoconferencing Systems 3510, 3520, 3525 and 3530 are vulnerable to (h).
- UploadServlet in Cisco Collaboration Server (CCS) running ServletExec before 3.0E are vulnerable to (i).

N1.3 CVE Entries

CVE-2004-0589, CVE-2004-0714, CVE-2004-1454, CVE-2005-2451, CVE-2005-2841, CVE-2005-2244, CVE-2004-0391, CVE-2004-1322, CVE-2005-0612, CVE-2004-0650

N1.4 How to Determine If You Are at Risk

The Cisco systems running without the patched versions of IOS referenced in the CVEs listed above are vulnerable. A network-management application, such as CiscoWorks (http://www.cisco.com/en/US/products/sw/cscowork/ps2425/) can ease IOS version auditing.

N1.5 How to Protect against These Vulnerabilities

Following are some common approaches to protect against these vulnerabilities:

- Apply access lists on all interfaces. These access lists should only allow the minimum of traffic necessary. Access lists on externally-facing interfaces should be especially stringent.
- Disable unnecessary services on the router or switch. View the running configuration of the router by using the **show running-configuration** command.
- If the system must run SNMP, try to run at least SNMP version 2, and preferably version 3. If possible, be sure to use SNMP signatures and encryption. On both versions 2 and 3, be sure to change the default SNMP community string. If possible, disable SNMP write access entirely. Many management applications need only read access to perform their functions.
- Be sure to run the latest available version of IOS that supports the necessary feature set.
- Disable Cisco Discovery Protocol if possible, as this allows for information disclosure and is contributory to vulnerability (f).

N1.6 References

http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp (Requires a Cisco account)
http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Hardening Cisco IOS Against Buffer Overflow Attacks
http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml

Cisco Security Advisories

a. Remote Denial-of-Service in BGP Processing
   http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml
b. Remote Denial-of-Service in SNMP Processing
   http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml
c. Remote Denial-of-Service in OSPF Processing
   http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml
d. Remote Code Execution in IPv6 Processing
   http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml
e. Remote Code Execution in Firewall Authentication Proxy
   http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml
f. Remote Code Execution in Cisco CallManager
   http://www.cisco.com/warp/public/707/cisco-sa-20050712-ccm.shtml
g. Hardcoded Username and Password in Cisco Wireless LAN Solution Engine
   http://www.cisco.com/warp/public/707/cisco-sa-20040407-username.shtml
h. Hardcoded SNMP Community Strings in Cisco IP/VC
   http://www.cisco.com/public/technotes/cisco-sa-20050202-ipvc.shtml
i. Remote Code Execution in Cisco Collaboration Server
   http://www.cisco.com/warp/public/707/cisco-sa-20040630-CCS.shtml
j. Cisco Devices IPSec Handling Vulnerabilities
   http://www.cisco.com/warp/public/707/cisco-sa-20051114-ipsec.shtml

N2. Juniper, CheckPoint and Symantec Products

N2.1 Description

Juniper's Operating System (JunOS) is Juniper's standard router OS. JunOS is the second most common backbone Internet router. CheckPoint and Symantec solutions like VPN and Firewalls also enjoy a wide deployment.

Vulnerabilities were announced during the last year in these products that could be exploited to reboot Juniper routers and compromise the Symantec and CheckPoint Firewall/VPN devices.

Exploit code is available for some of these flaws.

N2.2 Versions Affected

Juniper routers that are running an older JunOS version.
CheckPoint VPN-1/FireWall-1 NG with Application Intelligence R54, R55 or R55W
CheckPoint VPN-1/FireWall-1 Next Generation FP3
CheckPoint VPN-1/FireWall-1 VSX FireWall-1 G
Symantec Firewall/VPN Appliance 100, 200/200R (firmware builds prior to build 1.63)
Symantec Gateway Security 320, 360/360R (firmware builds prior to build 622)

N2.3 CVE Entries

CVE-2004-0467, CVE-2004-0468, CVE-2004-0699, CVE-2004-1474

N2.4 How to Protect against These Vulnerabilities

- Upgrade to the latest JunOS version for Juniper routers.
- Apply patches supplied by CheckPoint and Symantec.
- Disable "Aggressive Mode IKE" on VPN devices whenever possible.
- Audit network devices for default SNMP community strings. Scanners usually include SNMP testing suite with a variety of commonly used default community strings.

N2.5 References

Juniper OS Vulnerabilities
http://www.kb.cert.org/vuls/id/409555
http://www.kb.cert.org/vuls/id/658859
http://www.sans.org/newsletters/risk/display.php?v=4&i=4#widely3
http://www.sans.org/newsletters/risk/display.php?v=3&i=26#other5
http://secunia.com/advisories/17568

CheckPoint Advisories
http://www.checkpoint.com/techsupport/alerts/asn1.html
http://www.sans.org/newsletters/risk/display.php?v=3&i=30#widely2

Symantec Advisory
http://www.sarc.com/avcenter/security/Content/2004.09.22.html
http://www.sans.org/newsletters/risk/display.php?v=3&i=38#other1

N3. Cisco Devices Configuration Weaknesses

N3.1 Description

Cisco's Internetwork Operating System (IOS) provides a myriad of configuration options. There are several configuration options that are not secure by default. This document enumerates some of the more insecure default configurations on Cisco's IOS for the past year.

a. No Remote Logging By Default
b. Default SNMP Community Strings
c. Default or Nonexistent Default Passwords
d. IP Source Routing Enabled
e. TCP and UDP Small Services
f. Finger Service
g. IP Directed Broadcast Enabled
h. HTTP Configuration

N3.2 Versions Affected

As a rule, more recent versions of IOS have a more secure default configuration. However, even the most recent versions still are lacking certain security measures in their default configurations.

N3.3 How to Determine If You Are at Risk

Generally, it is necessary to know what version of IOS a device is running to determine its default configuration. A network-management application, such as CiscoWorks (http://www.cisco.com/en/US/products/sw/cscowork/ps2425/) can ease IOS version auditing. The running and saved configurations in IOS can be displayed with the **show running-config** and show startup-config commands, respectively.

N3.4 How to Protect against These Vulnerabilities

Following are some common approaches to protect against these vulnerabilities:

- Enable remote logging. To do this, make sure a secure syslog server is available. Configure the router to log to this device by issuing the **logging server *ip address*** and **logging on** commands.
- Disable SNMP if possible, or change the default community strings. SNMP can be disabled entirely with the **no snmp-server** command. For systems that need SNMP, the default community strings can be changed with the **snmp-server community** command. If possible, SNMPv3 should be used, and configured to use encryption and signatures.
- An encrypted enable (supervisor) password should be configured with the **enable secret** command. Passwords should also be set on the console, aux, and vty ports. Use the **password** command in the line configuration mode for each line. Line configuration mode can be accessed via the **line** command.
- IP Source Routing allows traffic originators to specify the path traffic will take through the network. This is generally not used for legitimate purposes on real networks, and should be disabled with the **no ip source-route** command.
- IOS provides numerous "small services" via TCP and UDP, such as echo and chargen. These services are generally not used and provide holes for potential attacks. They can be disabled with the **no service tcp-small-servers** and **no service udp-small-servers** commands.
- IOS provides a finger service to list the users currently logged into the router. This allows for information disclosure as well as a potential for attacks. It should be disabled with the **no service finger** command.
- IP Directed Broadcasts allow for unicast IP packets to be converted to link-layer broadcasts once they reach a specified subnet. These are generally only used maliciously, especially for so-called "smurf" attacks. Directed broadcasts should be disabled with the **no ip directed-broadcast** command.
- IOS allows for web-based configuration using an HTTP server embedded in the operating system. This HTTP server has been known to host security problems in the past, and is generally not needed. It should be disabled with the **no ip http** command.

N3.5 References

http://www.cisco.com/en/US/products/products_security_advisories_listing.html
http://www.cisco.com/warp/public/707/21.html

a. No Remote Logging By Default
   http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_r/frprt3/frtroubl.htm#1017943
b. Default SNMP Community Strings
   http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html
c. Default or Nonexistent Default Passwords
   http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0508
d. IP Source Routing Enabled
   http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Source_Routing/default.htm
e. TCP and UDP Small Services
   http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a008019d97a.shtml
f. Finger Service
   http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a008019d97a.shtml
g. IP Directed Broadcast Enabled
   http://www.netscan.org/broadcast/problem.html
h. HTTP Configuration
   http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/frprt1/frd1005.htm

Products For Identifying and Mitigating Top-20 Risks

1. Vulnerability Scanners and Patch Management Systems

- Microsoft Baseline Security Analyzer can be used for identifying vulnerable Windows systems.
- Open-source scanners as well as commercial vulnerability scanners and patch management systems are available from a number of vendors as well that can help identify vulnerable systems and/or automatically download patches to the vulnerable systems.

2. Intrusion Prevention/Detection Systems and Firewalls

- Network and Host-based Intrusion Prevention Systems can be used to prevent exploits targeted at vulnerabilities. These systems provide a "virtual" patch till the vendor patch is installed on the vulnerable systems.
- Network-based Intrusion Detection Systems can be used to alarm on suspicious network activity and exploits.
- Network-based Firewalls can be used to appropriately block the unwanted TCP/UDP ports at the network perimeter and inside.
- Host-based firewalls can be used to allow access to only selected services on a host.

3. Anti-virus and Malware Detection Software

- Anti-virus and Anti-spyware software can be used to remove viruses, spyware, adware, Trojans and backdoors from infected systems. Gateways running these software can be used to stop the malware from entering an organization.

The Experts Who Helped Create The Top-20 2005 List

Project Manager and Editor: Rohit Dhamankar, TippingPoint, a division of 3Com

Cesar Tascon Alvarez, Ernst and Young, Spain
Pedro Paulo Ferreira Bueno, Brasil Telecom
Arturo 'Buanzo' Busleiman, KTP Consultores, Argentina
David Chaboya, US Air Force
Anton Chuvakin, netForensics
Michel Cusin, Bell Security Solutions, Canada
Rhodri Davies, Vistorm, UK
Olivier Devaux, iSecureLabs
Sandeep Dhameja, Ambiron Trustwave
Gerhard Eschelbeck, Qualys
Edward Fisher, www.mentat.ws
John-Thomas Gaietto
Michele Guel, Cisco Systems
Mark Goudie, Data Networking Services, Australia
Kevin Hong, Korea Information Security Agency (KISA) and KrCERT/CC

Monty Ijzerman, McAfee, Inc.
Marcos A. Ferreira Jr., NXSecurity, Brazil
Rob King, TippingPoint, a division of 3Com
Alexander Kotkov, Perot Systems Corporation
Jean-Francois Legault, Bell Security Solutions, Canada
Rajesh Mony, Qualys
Russell Morrison, AXYS Environmental Consulting
Sanjay Pandit, DIRECTV
Leo Pastor, Advanced Consulting and Training, Argentina
Jeff Pike, Integrated Team Solutions Facility
Edward Ray, Netsec Design and Consulting
Chris Riley, Spherion
Christopher Rowe, Guilford Technical Community College
Jonathan Rubin, Dominion
Marc Sachs, SRI International and Internet Storm Center, SANS
Dinesh Sequeira, TippingPoint, a division of 3Com
Donald Smith, Internet Storm Center, SANS
Andrew van der Stock, OWASP
Luminita Vasiu, University of Westminster, UK
Koon Yaw Tan, Infocomm Development Authority of Singapore
Johannes Ullrich, Internet Storm Center, SANS
Rick Wanner
Team at AFENTIS Security, UK

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