Global Information Assurance Certification Paper

Windows Corporate Patch Management Without a Budget

Name: Doug Douillard

Certification: GIAC Security Essentials Certification (GSEC)
Version 1.4b, Option 1

Date Submitted: June 8, 2004

Abstract:

Windows client machines are often neglected when it comes to applying critical updates and patches. The days of allowing un-patched computers to remain on a network are long gone. Now an un-patched system can be exploited in a matter of seconds after being introduced to the Internet. The amount of time between the release of a patch and the introduction of the exploit is on the decline. The latest vulnerability related to a Windows critical update that has recently been exploited is the LSASS Vulnerability (MS04-011). The amount of time from patch to exploit was a record 18 days; this surpasses the previous record of 25 days held by the Blaster Worm. [1]

Unfortunately, many IT budgets do not account for security and patching procedures. Fortunately, there are many tools, techniques, and time saving tips that can help even the smallest security budget keep all computers up to date and patched. A patching procedure should be developed and maintained to ensure that a network maintains security. Software patching involves discovery, testing, deploying, scanning, & maintaining. I will mention techniques and tools that will help with the detection of missing updates, deploying the updates, and maintaining the patch process.

The Importance of Patching:

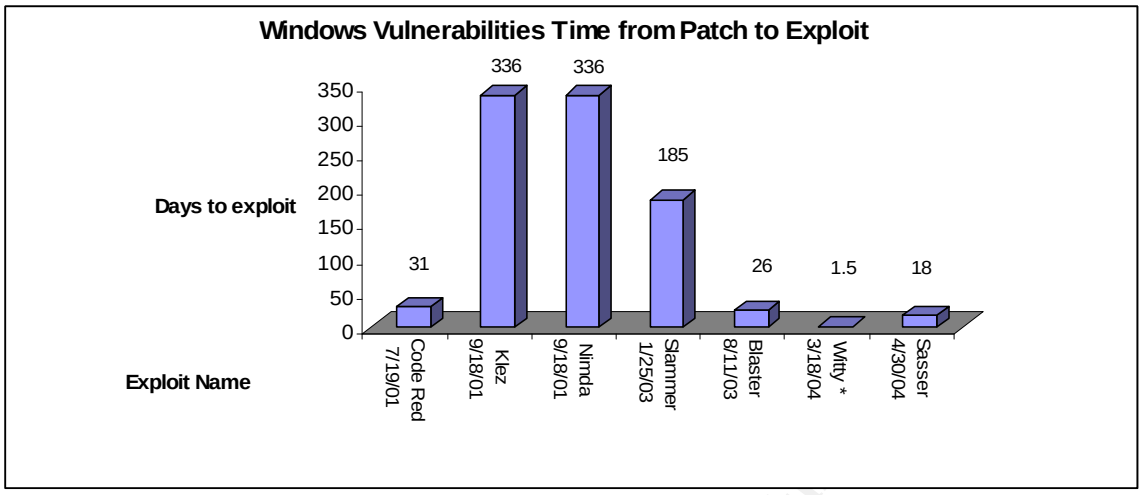
Network administrators need more than a firewall anymore, especially with mobile users. To achieve defense in depth, client side patching needs to be practiced. Vulnerabilities are appearing daily and are targeting the clients since they are often not updated as often as servers. Once the vulnerability is posted on the Internet it is just a matter of time before an exploit is released. Some exploits will directly infect a computer through the Internet or internal network if an infected machine enters the network. Exploits are taking less and less time to appear after a vulnerability has been reported. Often vendors may know about an exploit before the vulnerability is released to the public. The lack of having a patch developed in adequate time for the vulnerability can cause a zero-day attack which will cause the most damage. [2] The following graph displays some of the Windows vulnerabilities that have been exploited. The trend shows that the time from patch to exploit is decreasing. The Sasser Worm has the current shortest amount of time for a Windows vulnerability to be exploited with 18 days. Even though it is not a Windows vulnerability, the Witty Worm took only 36 hours for an exploit to be developed.[3]

---

[1] Pescatore, John; Nicolett, Mark. "Gartner First Take, "Rapid Sasser Attack Raises the Cost of Securing Windows". May 4, 2004. http://www4.gartner.com/resources/120800/120807/rapid_sasser_at.pdf

[2] Bradley, Tony. "Zero-Day Exploits". March 19, 2003. http://netsecurity.about.com/library/weekly/aa031903a.htm

[3] Schneier, Bruce. "The Witty worm: A new chapter in malware" June 02, 2004. http://www.computerworld.com/securitytopics/security/virus/story/0,10801,93584,00.html



(Fig 1) Windows Vulnerabilities Time from Patch to Exploit[4]

All clients should maintain up to date patches to ensure that they are not infected by exploits and viruses. Infected machines can have many drawbacks including, data loss, network downtime, security breaches, and they can take part in DDOS attacks. Distributed Denial of Service attacks will utilize many infected clients to attack web sites and cause the website to be unavailable for customers. On May 4th 2001 GRC.com was attacked by a DDOS and was shut down for over 17 hours. The attack utilized 474 zombie clients to fully immobilize the GRC.com website.[5] Denial of Service attacks can cause very significant impact to any business and cause a company a lot of money in downtime and lost profits.

Patching Technique:

Keeping up to date on security patches is a full time job. A patch management procedure should be well planned out and documented. By following a few steps you can be sure that your clients stay up to date with all the correct and valid software patches. A patching procedure should include the following:

- new patch identification
- patch testing
- test rollout
- full roll out
- Maintenance and scanning for missing patches

---

[4] Compiled from Riley, Steve. "What happens until you wait for exploit code". June 2, 2004. http://download.microsoft.com/download/6/b/d/6bd8e713-1a7c-489c-ab38-ea9b84a31955/2_SteveRiley.pdf & Symantec. "Symantec Security Response Expanded Threats". June 1, 2004. http://www.sarc.com/avcenter/vinfodb.html

[5] Gibson, Steve. "The Strange Tale of the Denial of Service Attacks Against GRC.com". October 6, 2004. http://grc.com/dos/grcdos.htm

* Witty Worm was an exploit for ISS's Black Ice products, not a Windows Vulnerability.

Besides the actual patch rollout, the first step of the patching procedure is probably the most important. The testing and deployment time can be drastically reduced if a new patch goes undiscovered for a time. With exploits being developed at a quickening pace, it is of the utmost importance to keep up to date on vulnerability and patch releases.

Microsoft has recently adjusted their patch deployment schedule to once a month for security bulletins. The Security bulletins will normally be released on the second calendar Tuesday of every month. An exception to the monthly release would occur if there is an immediate risk from attacks and malicious activities, then a patch would be released immediately.[6] Checking the Microsoft security website is highly advisable on a regular basis. The site should be checked on the second Tuesday of every month to determine new security risks. Administrators should also sign up for the Microsoft Security Notification Service. This service sends an email any time a new security patch is released from Microsoft.[6] To sign up for the free Security Notification Service, please visit http://register.microsoft.com/subscription/subscribeme.asp?ID=135. Microsoft also produces a monthly newsletter that provides valuable security information including security tips and Frequently Asked Questions. To sign up for this free newsletter please visit: http://www.microsoft.com/technet/security/secnews/default.mspx. Another way to keep up to date is to subscribe to RSS feeds. The feeder program sits in your system tray and checks websites for updates. This is a handy time saving tool so you don't need to check websites manually just to find that there isn't any new data posted on the site. There are free feed reader programs available on the Internet; check http://blogspace.com/rss/readers for some downloads. Some of the useful feeds include:

- Microsoft Security Bulletins: Http://www.microsoft.com/technet/security/bulletin/secrss.aspx
- Security Focus Vulnerabilities: http://www.securityfocus.com/rss/vulnerabilities.xml
- SANS Internet Storm Center: http://isc.sans.org/rssfeed.xml

There are many other useful RSS feeds available for free and paid subscription on the Internet.

It is also vital to keep informed of new vulnerabilities and exploits that may be released before vendors know about them. Many online newsgroups will discuss exploits and vulnerabilities and may post information before vendors release patches to repair the security flaws. Websites and newsgroups will provide feedback on patch successes and failures. Visiting patch information websites and newsgroups will help when you are testing new patches in a test environment. http://groups.google.com , http://www.ntbugtraq.com http://www.patchmanagement.org. Testing patches is a critical step in the

[6] Microsoft. "Standardizing the Patch Experience". June 1, 2004. http://www.microsoft.com/technet/security/topics/patch/stdpatex.mspx

patching life cycle. Rolling out a new patch before thoroughly testing it can have a devastating affect. An untested patch has the potential of causing network downtime or the loss of data and profits. There are a variety of methods to test patches, some will be more expensive to implement. For the best results a separate testing lab should be designed and utilized to fully test new patches.

To have the most success, your test environment should mimic your production environment as closely as possible. One of the most cost effective methods of achieving this would be to use virtual PC software. Both Microsoft and VMWare have virtual PC software available for under $200.[7] Both VMWare and Virtual PC 2004 have free trial versions available from their websites. Your testing environment should include all of the same hardware and software if possible. The test lab should also utilize the same patch deployment strategies as your production network. This will help ensure that the patches will also work in your production environment in a similar fashion as the test lab.[8] Once enough testing is established then the next phase of limited roll out can occur. During the testing phase as many possible client configurations should be tested to ensure patch stability in your production environment.

Before a mass roll out of the new patch can occur, limited live tests are necessary. "Software developers and other IT-savvy people make great guinea pigs because they're more sensitive to subtle problems that occur and they might be working with new code or applications that will soon be deployed."[9] One way to do a limited roll out is by using group policy and test OU's in an Active Directory environment. Login scripts and patching software are some of the other deployment methods available. Patch deployment methods will depend on your network layout and available patching software solutions. After the initial testing phase is complete, the main patch roll out can take place. Feedback from the beta testing group will help determine what types of problems may occur and how to fix the issues before rolling out patches. The whole testing phase may be a very short time frame or non existent depending on how crucial a patch is and if an exploit already exists for the patch. The amount of time to test a patch, is dwindling as the zero-day attack becomes more of reality and exploits are released at dizzying speeds. Once patches have been rolled out, continual maintenance and network scanning are required to catch machines that are vulnerable to an attack.

---

[7] VMWare. "VMWare Store". June 1, 2004. http://www.vmware.com/vmwarestore/pricing.html & Microsoft. "How to Buy Virtual PC 2004" June 1, 2004. http://www.microsoft.com/windowsxp/virtualpc/howtobuy/default.asp

[8] Fossen, Jason. "Patch Testing". April 2004. http://www.winnetmag.com/Windows/Article/ArticleID/41979/41979.html

[9] Fossen, Jason. "Patch Testing". April 2004. http://www.winnetmag.com/Windows/Article/ArticleID/41979/41979.html

A Few Free Utilities:

There are a variety of free utilities available to check for missing patches and vulnerabilities. I will mention three of the tools here, one each from Microsoft, Shavlik, and GFI. Both HFNetChk by Shavlik, and Languard by GFI, have full featured versions of their free tools available for purchase. Microsoft's Baseline Security Analyzer or MBSA, is based on HFNetChk and is available for free from Microsoft.

MBSA is a graphical analyzer that works with Windows NT 4 and later operating systems. This tool can scan a single computer or multiple computers and report a variety of information. MBSA 1.2 will report missing patches for the operating system, IIS, Exchange, Office, MDAC, Internet Explorer, Windows Media Player, Biz Talk, Commerce Server, CM Server, and Host Integration Server. MBSA will also report other OS information and vulnerabilities like password policies and anonymous access settings.[10] This utility is a great starting place to determine if a computer has any missing patches and a quick list of possible vulnerabilities. See Figures 2 & 3 for example screen shots.

MBSA also has scripting capabilities to fully automate the scanning process. The command line version is very versatile and has a variety of switches that will allow customization of the scanning process. Running MBSACLI /? at the command line will display all switches and give examples of scripts to scan computers. For example running the following script will scan the domain MYDOMAIN for vulnerabilities and missing patches and redirect the output to d:\MBSA\scan.txt. *MBSACLI /d MYDOMAIN /f "d:\MBSA\scan.txt*". MBSA requires administrative rights to scan computers so you will need to be a member of the local admin group on each machine scanned or be a member of the domain administrator group.[11] Using task scheduler a script can be run with the appropriate rights to scan any number of computers with a variety of options.

MBSA is based on Shavlik's HFNetChk program for patch scanning. HFNetChk Pro scans for missing patches like MBSA, but HFNetChk will also deploy the missing patches to the scanned computers. (Fig 4) Unlike MBSA, HFNetChk only scans for patches and doesn't show the windows vulnerabilities that MBSA does. HFNetChk Pro also has Graphical and command line options to fully automate the patch scanning process. Running HFNETCHK4PRO /? At the command line will display all of the command switches available. The switches are very similar to the switches available for MBSA.
For example running the following script will scan the domain MYDOMAIN for missing patches and save the output to d:\hfnetchk\scan.txt. *hfnetchk4pro –d*

[10] Microsoft. "White Paper: Microsoft Baseline Security Analyzer V 1.2". February 20, 2004. http://www.microsoft.com/technet/security/tools/mbsawp.mspx
[11] Microsoft. "White Paper: Microsoft Baseline Security Analyzer V 1.2". February 20, 2004. http://www.microsoft.com/technet/security/tools/mbsawp.mspx

mydomain –f "d:\hfnetchk\scan.txt". Some of the available switches can use files to select which clients get scanned, supplying a password and username, and how brief or lengthy the output is displayed.
A task scheduling option is included with the graphical version to allow scheduled scans and patch deliveries. The command line version can be automated using the task scheduler within Windows. The trial version of HFNetChkPro provides unlimited scanning and deployment of patches to 10 workstations and one server. [12]

GFI's LANGuard also has a patch scanning utility that is available for free. LANGuard also adds many security scanning and computer information options that makes it a very useful tool for network administrators. The full version of LANGuard will also allow patch deployment, the freeware version will let you scan 25 workstations and deploy patches for a 60 day trial period.[13] LANGuard will return many useful pieces of information about clients that it can contact. Missing patches and vulnerabilities are included, but LANGuard will also report open ports and running processes to help see if computers are running file sharing programs or may be open for an outside attack. Windows services, open sessions, and shares with permission settings will help keep a machine well protected from unwanted traffic. (Fig 2) LANGuard is definitely a great utility that gives an administrator a great deal of control of workstation computers. Some of the other controls include Microsoft and custom patch delivery, auditing control, power shutdown. LANGuard also provides report creation and baseline checking to determine trends and to create a scanning history. The pricing on the full version of LANGuard is very reasonable and the free version will allow scanning of 25 computers at a time.

Patch Delivery:

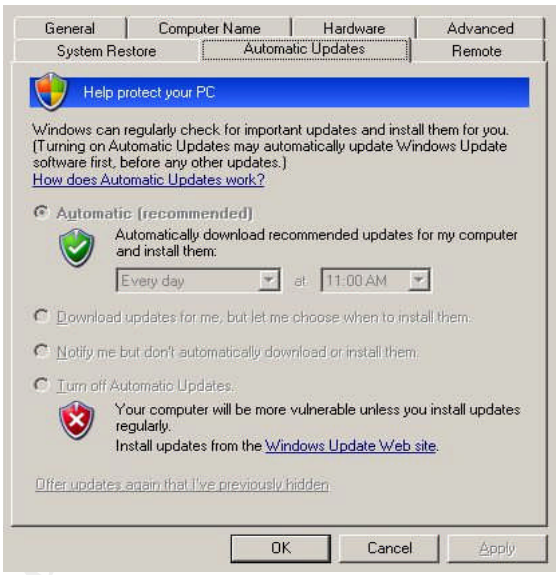
Knowing about patches and testing the patches is one thing, but getting the patches out to the required computers before they are exploited can be a tricky process. Microsoft has a few free options to help with the patch delivery problem. Following I will mention Microsoft's two options of Windows update and Software Update Services. There are also scripting options which are invaluable if a computer needs to be updated without getting on a network. Some 3rd party patching tools include the previously mentioned HFNetChk and LANGuard.

Windows update is Microsoft's well known update tool for the Windows Operating System. This tool is the website http://windowsupdate.microsoft.com which checks a machine for missing patches and will download and install missing patches, updated windows features, and drivers. Windows Update is a good tool for updating single computers either manually or with the automatic

[12] Shavlik. "HFNetChkPro 4.0 The Next Generation in Patch Management". June 1, 2004. http://www.shavlik.com/pHFNetChkPro.aspx
[13] GFI. "LANGuard Network Security Scanner – Freeware version" June 1, 2004. http://www.gfi.com/lannetscan/lanscanfreeware.htm

updates feature. Computers in a corporate domain can also utilize automatic updates to keep up to date. By using Group Policy in an active directory domain, automatic updates can be set on clients to contact the Windows Update site and get updates.

The automatic updates client software is included with Windows. Computers can be set to contact the update server automatically, to download the updates and prompt the user to install, notify the user before downloading or, turn automatic updates off. Clients contacting Windows Updates could cause a network bottleneck if a corporation has a slow dedicated Internet connection. Another problem with using Windows Update is the lack of internal testing of new patches. Since Windows Update will display new patches as they are released, an un-tested patch may cause problems on computers that have specialized settings and software.



(Fig 5) Windows XP Automatic update client.

One solution to test patches before delivery is through the use of scripting. By using batch files updates can be delivered to clients after the patches have been tested. Microsoft provides a program called Qchain to string all needed updates into one installation only requiring one reboot. The completed batch file can be distributed to clients in a variety of ways. Group Policy and login scripts could automatically deploy the updates to clients. Manual options could include users clicking a batch file from a network location or use a CD containing the updates. By running the batch file from a CD so that a network connection isn't needed. This type of distribution is handy to ensure that a new machine is not vulnerable once it is introduced to a network. Also machines that have been compromised can get the updates they need without needing to have network access.

Here is an example of batch file utilizing Qchain and a program called osver by Bill Stewart to determine the service pack level.[14] This script is set to determine the CD drive and run from the CD, if windows XP service pack 1 is installed then the hotfixes will run. This is a simple script that would run from a CD and will install the listed hotfixes even if they are already installed.

[14] Stewart, Bill. "Admin Script Tools (OSVER utility)". February 27, 2004. http://home.comcast.net/~stewartb/wast.html

```
@echo off
set cdrom=none
if exist d:\bootcd.id set cdrom=d:\
if exist e:\bootcd.id set cdrom=e:\

for /f "Tokens=*" %%s in ('osver -s')   do set sp="%%s"
if %sp% == "Service Pack 1" goto XPhotfix
%cdrom%\WindowsXP\xpsp1a_en_x86.exe -u -n -z

:XPhotfix
%cdrom%\WindowsXP\WindowsXP-KB810217-x86-ENU.exe -u -z
%cdrom%\WindowsXP\WindowsXP-KB823182-x86-ENU.exe -u -z
%cdrom%\WindowsXP\WindowsXP-KB826939-x86-ENU.exe /passive /norestart
%cdrom%\WindowsXP\WindowsXP-KB828035-x86-ENU.exe /passive /norestart
%cdrom%\qchain.exe
```

Script is structured similar to scripts available from Microsoft.[15]

A more complex script could be created to utilize HFNetChk or Qfecheck to see if patches are already installed. Doc Rice has a good example of a script utilizing Qfecheck at http://winpatch.homeip.net/index.html[16]

Microsoft has updated their patch deployment and has changed the switches available with the update.exe program. Two new switches allow for integrating patches and uninstalling patches. The script listed above includes patches that utilize the older version of update.exe and the new version. Using the passive or u switch will show the display on screen, but will not allow user interaction. The user will be prompted to restart once all of the hotfixes have been installed. A full list of available switches is available from Microsoft support.[17] Creating batch files and delivering them to clients can be a tedious and time consuming task. This need for testing patches and automating patch delivery, lead to the creation of Software Update Services or SUS.

SUS is Microsoft's answer to Windows Update in the corporate environment. SUS runs on a central server in a domain and delivers patches to computers on a predetermined schedule. Clients will contact the server and get patches directly from the local network instead of going to windows update. The automatic update client software is included in Windows XP service pack 1 and Windows 2000 service pack 3. SUS clients must be either Windows XP or Windows 2000 with Service pack 2. If needed, the client software is included

---

[15] Microsoft. "Microsoft Knowledge Base Article - 296861 How to Install Multiple windows Updates or Hot fixes with only one reboot". March 22 2004. http://support.microsoft.com/?kbid=296861

[16] Rice, Doc. "Security Patch Scripts for Microsoft Windows NT 4.0/2000/XP". April 13, 2004. http://winpatch.homeip.net/index.html

[17] Microsoft. "Microsoft Knowledge Base Article - 262841 Command-Line Switches for Windows software update Packages". April 15, 2004. http://support.microsoft.com/default.aspx?scid=kb;EN-US;262841

with SUS or it can be downloaded at http://www.microsoft.com/sus. The following are the requirements for the Software Updates Services server. This configuration will support approximately 15,000 clients.[18]

- Windows 2000 Server service pack 2 or greater or Windows 2003
- Pentium III 700 MHz or higher processor
- 512 Megabytes of RAM
- 6 Gigabytes free of space for security updates and setup
- IIS (IIS lockdown tool is installed and configured automatically)

Installing SUS is a quick process and the default setting will use the current server name as the SUS server name. After downloading the SUS software and running through the installation the SUS Admin site is loaded. (Fig 6) The first thing to do is set up a synchronization schedule. Choose a time when the network will be the least active, like 3AM. After first installing SUS you will need to select synchronize now to get all of the updates. After synchronization is complete, the updates will need to be approved. By clicking on the approve updates link a list of all updates will be listed. Select the updates that you want to approve and click approve. Only the updates that are approved will be installed to clients, this will allow the administrator time to test new patches as they are released.

The clients can be setup to contact the SUS server through group policy. The administration template that is included with SUS 1.0 has four options that can be set using group policy.

Policy	Setting	Definition
Configure Automatic Updates	2 – Notify for Download & notify for install 3 – Auto download & notify for install 4 – Auto download & Schedule Install Scheduled date & time	Use 4 as the setting for a completely automatic download and install
Specify intranet Microsoft update service location	Type in the name of the SUS server http://mysus Set Internet statistics server to the SUS server	The name of the SUS server that the clients will connect to.
Reschedule Automatic Updates scheduled installation	Wait after system startup (minutes)	How long to wait after startup if the computer missed the installation schedule
No auto-restart for scheduled Automatic Updates installations	Enabled or disabled	The computer will prompt the user to reboot.

[18] Microsoft. "Software Update Services Deployment White Paper". January 19, 2004. page 7. http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx

(Fig 7) wuau.adm group policy template for SUS 1 (compiled from wuau.adm)

When using group policy separate OU's can have different install times. Setting different install times may help network congestion when patches are deployed.

The SUS settings can also be installed on the clients through scripting and using .reg files if an active directory environment is not available. The registry file can be exported from a computer that has already been setup for SUS through group policy or created from scratch. The following registry file will cause the client to contact the SUS server mysus at 11pm everyday. The client will automatically download and install any new updates, the client will then be prompted to reboot. If a scheduled installation is missed the client will contact the SUS server 1 minute after it has been started up.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUp
date]
"WUServer"="http://mysus"
"WUStatusServer"="http://mysus"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUp
date\AU]
"NoAutoRebootWithLoggedOnUsers"=dword:00000001
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000004
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000023
"UseWUServer"=dword:00000001
"RescheduleWaitTime"=dword:00000001
```

One thing that is lacking in SUS 1.0 are reporting options, the IIS logs need to be looked at to determine further information about installations and problems. Many SUS administrators have developed their own utilities that will provide reporting for SUS. A great website to find SUS tools, news, and forums is http://www.susserver.com.[19] In the forums there are many links to reporting utilities. After using many of the reporting utilities found on susserver.com I feel that the best free reporting option is the one provided by the user stappel. Stappel's reporting tool SUSReports can be downloaded and viewed at http://193.78.132.15/.[20] (fig 8) This reporting tool uses either SQL or MySql to parse the IIS logs. Then IP address, Client name, last active, OS version, patch download and installation numbers, errors, and log files can be viewed. Using one of these reporting options will help in determining client installation failures and successes. A few other problems with SUS include the inability to uninstall

[19] Kornman, Scott. "SUSServer Forums". June 1, 2004. http://www.susserver.com

[20] Stappel. "SUS Reports" June 1, 2004. http://193.78.132.15/

patches and not being able to isolate patches to separate groups of clients. Microsoft has been improving on SUS and is scheduled to release SUS 2.0 or Windows Update Services (WUS) sometime in late 2004.[21]

After using the WUS beta, it is a significant update of SUS 1.0. The new Windows Update Service utilizes the new BITS client and the new MSI version 3 to deliver patches to clients. "The new delta compression scheme will eventually make MSI 3.0—based patches as much as 90 percent smaller than equivalent patches released today."[22] WUS also delivers patches for Office products and some server side products. Clients can be separated into groups and patches can be delivered to these groups or to all groups. The reporting options included in WUS allow administrators to view any number of reports about clients. Figure 9 shows a screenshot of an overview of patches installed on clients. The WUS group policy tool is included with Windows XP Service Pack 2 and provides an additional 7 options over the wuau.adm included with SUS 1.0.

- Do not display 'Install Updates and Shut Down'. Option in shut down windows dialog box. Removes the 'install and shut down' option in the shut down windows dialog box. (requires XP SP2)

- Do not adjust default option to 'Install Updates and Shut Down' in shut down windows dialog box. 'Install updates and shut down' option is allowed to be the default choice. (requires XP SP2)

- Enable client-side targeting. Specifies the target group name that should be used to receive updates from an intranet Microsoft update service.

- Automatic updates detection frequency. Specifies the hours that windows will use to determine how long to wait before checking for available updates. Default is 22 hours if not set or disabled.

- Allow automatic updates immediate installation. Specifies whether automatic updates should automatically install certain updates that neither interrupt windows services nor restart windows.

- Delay restart for scheduled installation. Specifies the amount of time for automatic updates to wait before proceeding with a scheduled restart. If disabled or not configured the time is 5 minutes.

[21] Microsoft. "Software Update Services 2.0 Overview". June 1, 2004. http://www.microsoft.com/technet/security/guidance/sus_2_0_overview.mspx

[22] Thurrott, Paul. "What you need to know about Windows Update Services". April 2004. http://www.winnetmag.com/Articles/Print.cfm?ArticleID=41969

- Re-prompt for restart with scheduled installations. Specifies the amount of time for automatic updates to wait before prompting again with a scheduled restart. If disabled or not configured the time is 10 minutes.

(List compiled from wuau.adm included with Windows XP Service Pack 2 RC1)

Windows Update Services will include many new features and will be a benefit to any environment that needs a patching solution. WUS will also include on demand installations to force updates to clients.[23] This added benefit of forcing critical updates will definitely help when patches need to quickly delivered in the wake of exploits.

Other software options for patch delivery include LANGuard and HFNetChk. The pricing model for these products falls out of the free range, but they both provide additional extras that may make them worth the cost. As well as patch scanning options, they both provide on demand patch delivery options. The table in figure 10 states prices for both LANGuard and HFNetChk as quoted from their websites as of June 1, 2004.[24]

IP Addresses	HFNetChk Pro version 4.0	LANGuard N.S.S version 5.0
25	$620.00	$315.00
50	$1,220.00	$395.00
100	$2,080.00	$495.00
Unlimited	Contact Shavlik	$995.00 *

* per administrator
(Fig 10) Pricing for LANGuard and HFNetChk

LANGuard goes a few steps beyond the patch management realm and provides a many layered defense in depth scanning tool. LANGuard will report the following information:

- missing security patches
- potential vulnerabilities
- open shares
- open ports
- active sessions
- services/applications active on the computer
- key registry entries
- weak passwords

[23] Microsoft. "Windows Update Services - beta version overview". June 1, 2004. http://download.microsoft.com/download/3/d/e/3de7e695-109a-494f-b43a-5cb8f7f98293/WinUS_Datasheet.doc

[24] Shavlik. "Shavlik Technologies Online Store". June 1, 2004. http://www.digitalriver.com/dr/v2/ec_Main.Entry?SP=10007&SID=48005&CID=0&CUR=840&DSP=0&PGRP=0&CACHE_ID=0 & GFI. "GFI LANGuard Network Security Scanner – Pricing" June 1, 2004. http://www.gfi.com/pricing/pricelist.asp?product=lanss

- users and groups

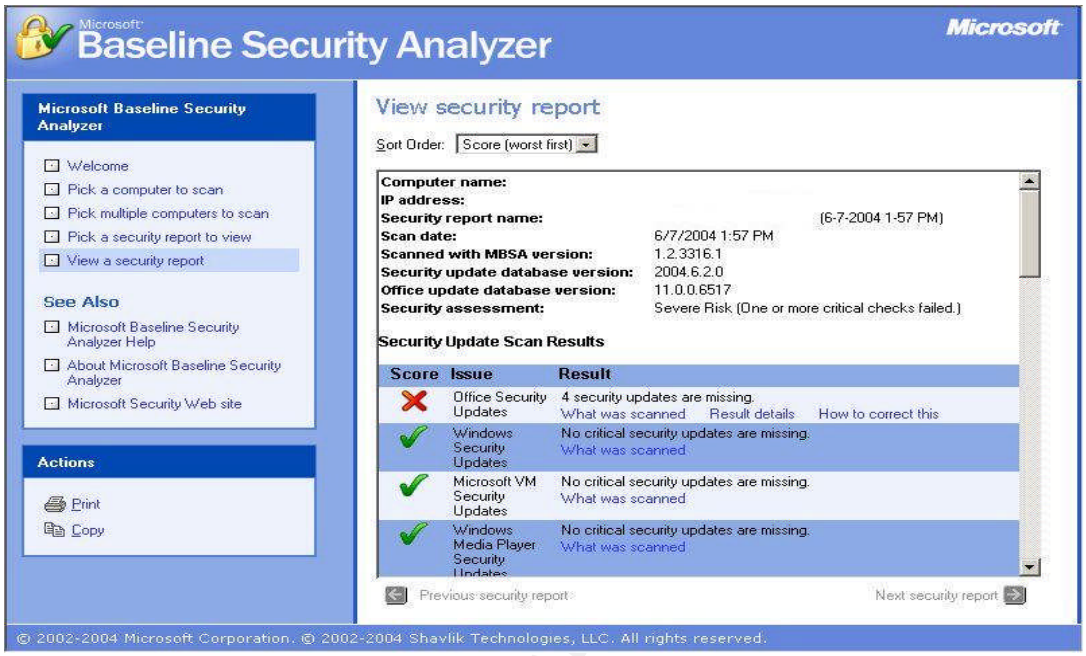
Using LANGuard and SUS together can improve the functionality of both products. SUS can push out Windows patches and service packs on a scheduled basis to the domain. LANGuard can then be used to scan the network to ensure that the patches are installed and if there are any other vulnerabilities on client machines. LANGuard can install patches on demand if a patch needs to be installed immediately and can not wait for the SUS scheduled install time. LANGuard has been voted #1 Windows security scanner NMAP users & over 200,000 GFI customers.[25] If LANGuard is not in the budget, MBSA and SUS can make a good replacement. Patches can be pushed out to clients with SUS and then verified to be installed with MBSA.

Conclusion:

Patch management is critical and should be planned out and followed. The time frame from vulnerability to exploit is quickly decreasing. It is critical to have a patch management procedure in place and practiced. A definite patching process including identification, testing, delivery, and scanning should be practiced. Microsoft has some options if there isn't a budget for patch management. Using MBSA to scan for missing updates and SUS to deploy the patches is a cost effective approach to keeping clients up to date. If the budget allows, utilizing LANGuard with a SUS server will create a total security scanning package. When the next Windows exploit hits, you will be ready for it.

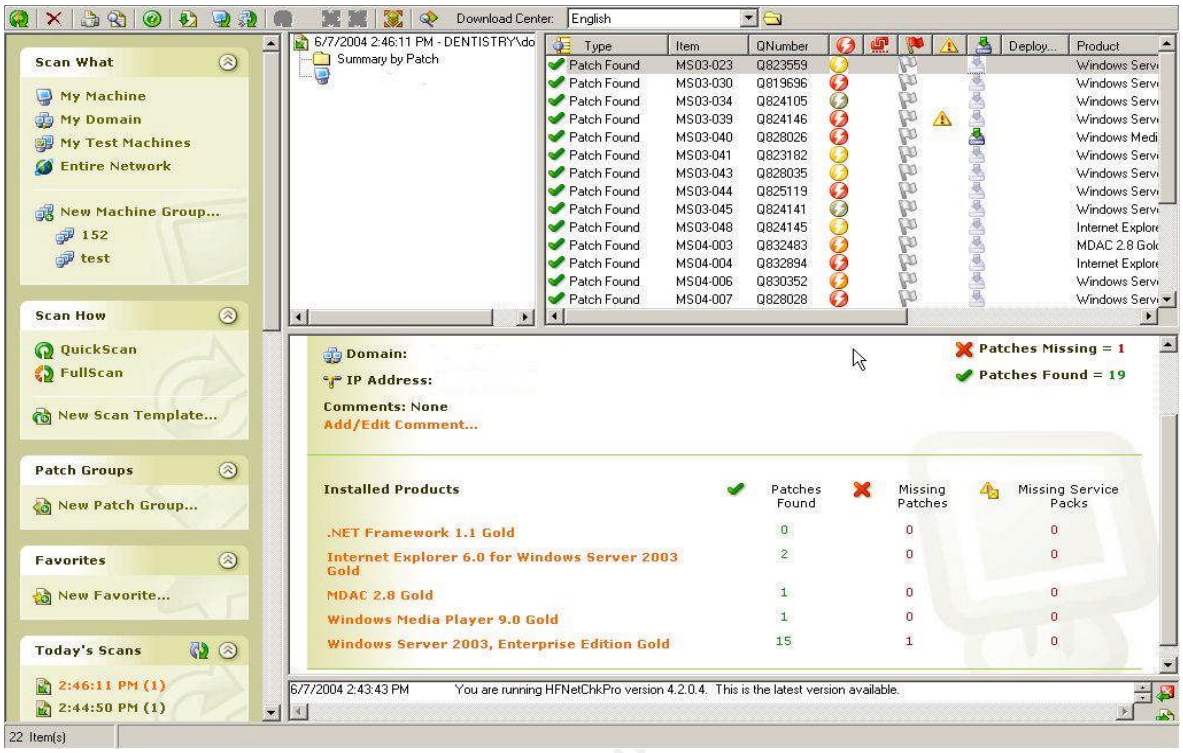
[25] GFI. "LANGuard Network Security Scanner". June 1, 2004. http://www.gfi.com/lannetscan/

Appendix:

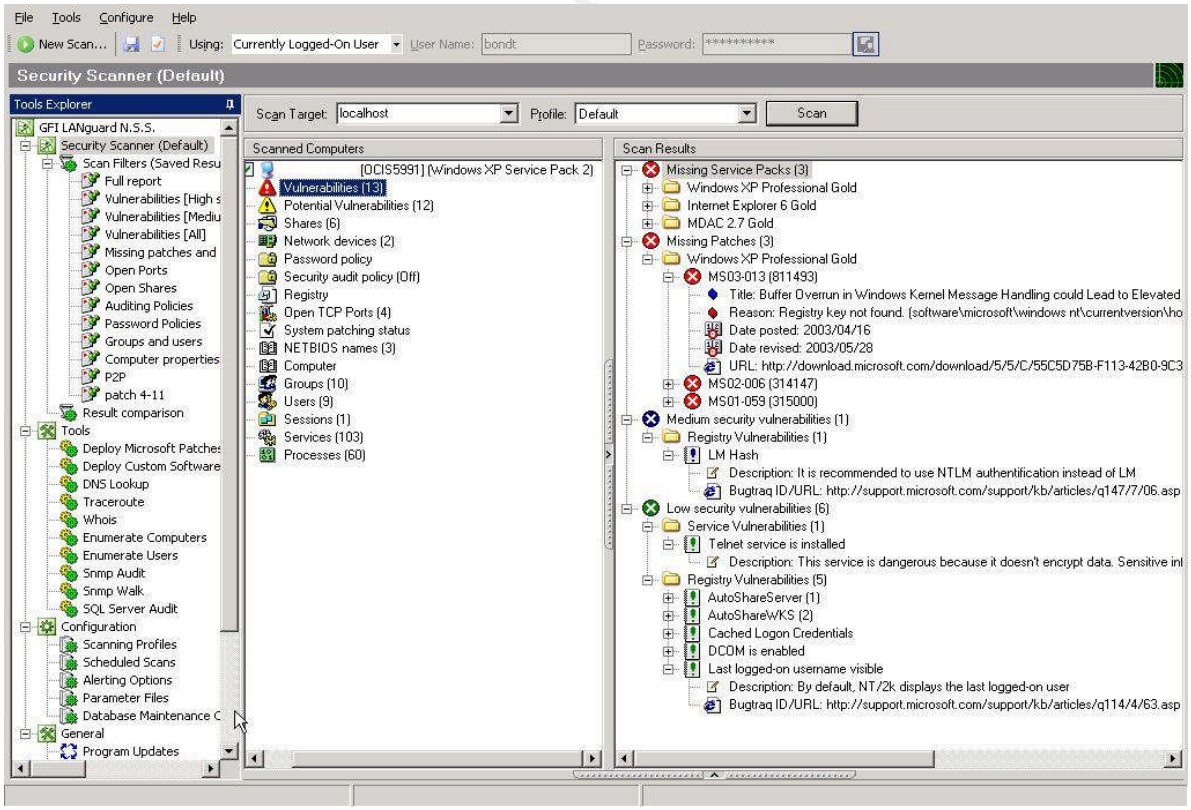


(Fig 2) MBSA scan showing security update scan results

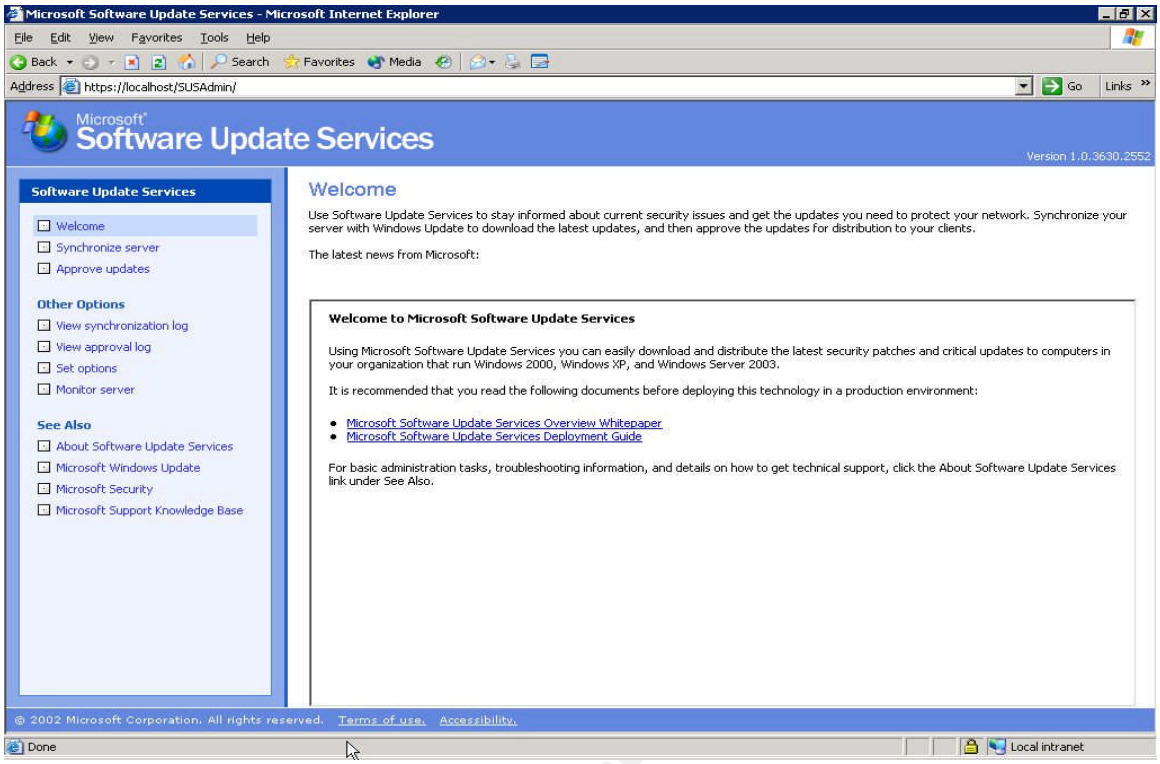
(Fig 3) MBSA scan showing Vulnerabilities scan results.



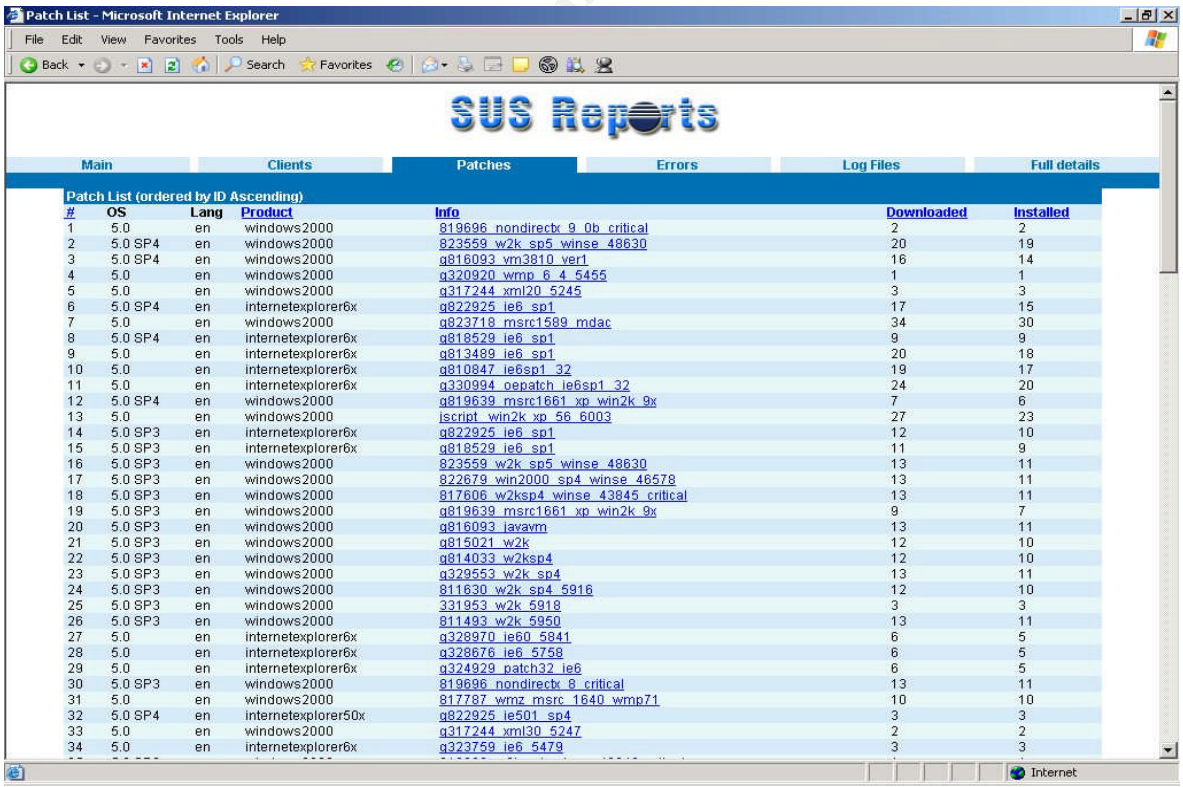
(Fig 4) HFNetChk 4.0 scan showing patch status.



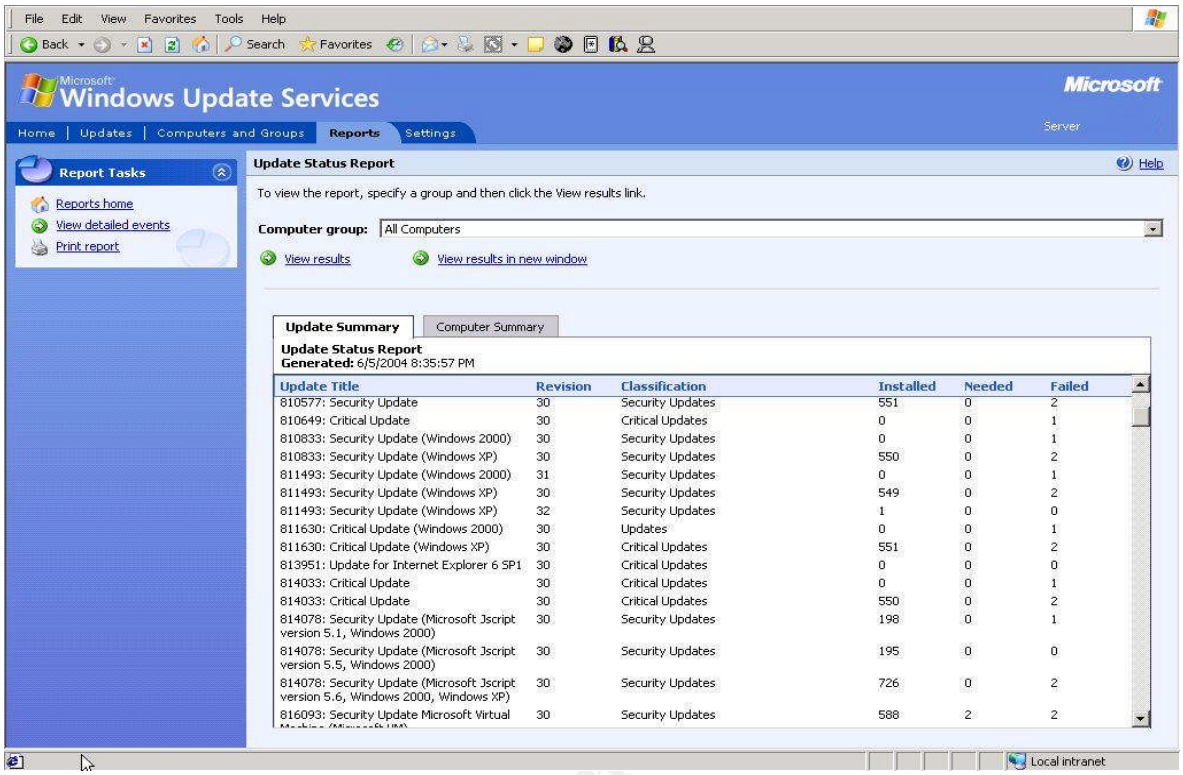
(Fig 5) LANGuard scan of the localhost showing vulnerabilities in the scan results window.



(Fig 6) Software Update Services Admin page



(Fig 8) SUS Reports free reporting utility.



(Fig 9) WUS Beta report showing an update summary of patch activity on clients.

Glossary

Bradley, Tony. "Zero-Day Exploits". March 19, 2003. http://netsecurity.about.com/library/weekly/aa031903a.htm

FAQ, JSI. "FAQ 5082 - How do I identify and apply Microsoft updates and hotfixes after you install Windows 2000 Professional on your computer?" June 1, 2004. http://www.jsiinc.com/SUBK/tip5000/rh5082.htm

Fellinge, Jeff. "Patching Windows with SUS". March 2003. http://www.winnetmag.com/Article/ArticleID/37938/37938.html

Fontana, John. "NetworkWorldFusion - "How to handle Patch Management"". December 1, 2003. http://www.nwfusion.com/research/2003/1201howtopatch.html

Fossen, Jason. "Patch Testing". April 2004. http://www.winnetmag.com/Windows/Article/ArticleID/41979/41979.html

GFI. "LANGuard Network Security Scanner". June 1, 2004. http://www.gfi.com/lannetscan/

GFI. “LANGuard Network Security Scanner – Freeware version” June 1, 2004. http://www.gfi.com/lannetscan/lanscanfreeware.htm

GFI. “GFI LANGuard Network Security Scanner – Pricing” June 1, 2004. http://www.gfi.com/pricing/pricelist.asp?product=lanss

GFI. "Patch Management with GFI LANGuard N.S.S & Microsoft SUS". June 1, 2004. http://www.gfi.com/whitepapers/patch-management.pdf

GFI. "Using GFI LANGuard Network Security Scanner to secure your Internal Network". June 1, 2004. http://www.gfi.com/whitepapers/lannetworkscanner.pdf

Gibson, Steve. “The Strange Tale of the Denial of Service Attacks Against GRC.com”. October 6, 2004. http://grc.com/dos/grcdos.htm

Kornman, Scott. "SUSServer Forums". June 1, 2004. http://www.susserver.com

Microsoft. "Microsoft Knowledge Base Article - 296861 How to Install Multiple windows Updates or Hot fixes with only one reboot". March 22 2004. http://support.microsoft.com/?kbid=296861

Microsoft. "Software Update Services Deployment White Paper". January 19, 2004. 93 pages. http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx

Microsoft. "Microsoft TechNet chat forum "Microsoft Windows Update Services Server"". May 19, 2004. http://www.microsoft.com/technet/community/chats/trans/windowsnet/wnet0519.mspx

Microsoft. "Understanding Patch and Update Management: Microsoft's Software update strategy". October 2003. http://www.microsoft.com/security/whitepapers/patch_management.asp

Microsoft. "Standardizing the Patch Experience". June 1, 2004. http://www.microsoft.com/technet/security/topics/patch/stdpatex.mspx

Microsoft. "Revamping the Security Bulletin Release Process". November 15, 2003. http://www.microsoft.com/technet/security/bulletin/revsbwp.mspx

Microsoft. "Microsoft Security Guidance Center: Patch Management Index". June 1, 2004. http://www.microsoft.com/security/guidance/topics/PatchManagement.mspx

Microsoft. "Software Update Services 2.0 Overview". June 1, 2004. http://www.microsoft.com/technet/security/guidance/sus_2_0_overview.mspx

Microsoft. "Windows Update Services - beta version overview". June 1, 2004. http://download.microsoft.com/download/3/d/e/3de7e695-109a-494f-b43a-5cb8f7f98293/WinUS_Datasheet.doc

Microsoft. "Microsoft Knowledge Base Article - 328010 How to configure automatic updates by using Group Policy or registry settings". April 27, 2004. http://support.microsoft.com/?kbid=328010

Microsoft. "How to Buy Virtual PC 2004" June 1, 2004. http://www.microsoft.com/windowsxp/virtualpc/howtobuy/default.asp

Microsoft. "Microsoft Security Notification Service". October 1, 2003. http://www.microsoft.com/technet/security/bulletin/notify.mspx

Microsoft. "White Paper: Microsoft Baseline Security Analyzer V 1.2". February 20, 2004. http://www.microsoft.com/technet/security/tools/mbsawp.mspx

Microsoft. "Microsoft Knowledge Base Article - 262841 Command-Line Switches for Windows software update Packages". April 15, 2004. http://support.microsoft.com/default.aspx?scid=kb;EN-US;262841

Pescatore, John; Nicolett, Mark. "Gartner First Take, "Rapid Sasser Attack Raises the Cost of Securing Windows". May 4, 2004. http://www4.gartner.com/resources/120800/120807/rapid_sasser_at.pdf

Petri, Daniel. "Why use the combination of GFI LANGuard N.S.S and Microsoft SUS server?" May 13, 2004. http://www.petri.co.il/gfi_languard_nss.htm

Rice, Doc. "Security Patch Scripts for Microsoft Windows NT 4.0/2000/XP". April 13, 2004. http://winpatch.homeip.net/index.html

Riley, Steve. "What happens until you wait for exploit code". June 2, 2004. http://download.microsoft.com/download/6/b/d/6bd8e713-1a7c-489c-ab38-ea9b84a31955/2_SteveRiley.pdf

Schneier, Bruce. "The Witty worm: A new chapter in malware" June 02, 2004. http://www.computerworld.com/securitytopics/security/virus/story/0,10801,93584,00.html

Shavlik. "HFNetChkPro 4.0 The Next Generation in Patch Management". June 1, 2004. http://www.shavlik.com/pHFNetChkPro.aspx

Shavlik. "Shavlik Technologies Online Store". June 1, 2004. http://www.digitalriver.com/dr/v2/ec_Main.Entry?SP=10007&SID=48005&CID=0&CUR=840&DSP=0&PGRP=0&CACHE_ID=0

Symantec. "Symantec Security Response Expanded Threats". June 1, 2004. http://www.sarc.com/avcenter/vinfodb.html

Stappel. "SUS Reports" June 1, 2004. http://193.78.132.15/

Stewart, Bill. "Admin Script Tools (OSVER utility)". February 27, 2004. http://home.comcast.net/~stewartb/wast.html

Thurrott, Paul. "What you need to know about Windows Update Services". April 2004. http://www.winnetmag.com/Articles/Print.cfm?ArticleID=41969

VMWare. "VMWare Store". June 1, 2004. http://www.vmware.com/vmwarestore/pricing.html