# Global Information Assurance Certification Paper

Harold Pasini
April 7, 2003

GIAC Security Essentials Practical v1.4(b), Option 1

# EFFECTIVE PATCH MANAGEMENT IN A MICROSOFT ENVIRONMENT

## I. ABSTRACT

Systems are becoming more complex and numerous on the Internet, a trend which lends itself to the introduction of a greater number of vulnerabilities. Hackers become aware of vulnerabilities immediately and are ready to exploit them at their first opportunities. As a result, thorough patch management has become a required function of any proper system management. In the past, Microsoft has not made this job easy. This paper intends to help guide system administrators through the development of a patch management plan, with a focus on Microsoft systems.

## II. THE GROWING WORLD OF VULNERABILITIES

As software becomes more complex through the years, the number of potential vulnerabilities grows exponentially. Microsoft Windows 3.1 contained approximately 3 million lines of code. In contrast, Microsoft Windows 2000 contains over 50 million lines of code. With an estimated 5 to 20 bugs per thousand lines of code in published software, it is easy to see that the potential for undiscovered vulnerabilities to exist in production servers is staggering. The number of vulnerabilities reported to CERT rose from 311 in 1997 to 4,129 in 2002. Accordingly, the number of security alerts and notes published rose from 50 in 1997 to 422 in 2002.

The vast number of vulnerabilities in software around the world creates a virtual playground for hackers. As the number of systems connected to the Internet grows, so does the playground. The number of hosts advertised in the Domain Name Service rose from approximately 16 million in 1997 to more than 171 million in 2003. It is estimated that there were over 605 million people on the Internet worldwide as of September 2002.

It is no surprise that, as the number of people and systems on the Internet grow and the number of vulnerabilities in software grows, the number of security incidents on the Internet is also growing at an alarming rate. This can be seen by the number of incidents reported to CERT, which rose from 2,134 in 1997 to 82,094 in 2002.

Microsoft plays a key role in this security playground. Their market share in the server marketplace has risen from 42 percent in 2000 to 49 percent in 2001, according to a report from IDC Research. This growth makes Microsoft operating systems an appealing target for hackers.

### The Role of Patch Management

While firewalls, anti-virus software, and intrusion detection systems are important in the fight to secure an enterprise, these tools do not negate the need for proper patch management. Vulnerabilities can easily be exploited through a hole in a firewall. A trusted source can inadvertently provide files carrying a dangerous payload. In many cases, by the time an intrusion is detected, valuable data may have already been lost or stolen.

With the onslaught of vulnerabilities and people waiting to exploit them, the importance of patching vulnerabilities has become crucial. At the same time, the cost of staying on top of such vulnerabilities has skyrocketed, both financially and personnel-wise. The Aberdeen Group estimates that companies spend over $2 billion annually on patch management, with an average of four full-time IT staff members for every 10,000 employees. The Gartner Group predicts that through 2005, 95 percent of cyber attacks will exploit security holes for which patches have already been published. The SQL Slammer worm, which was introduced on January 26, 2003, exploited a vulnerability which was identified six months earlier. A patch published on July 24, 2002 would have stopped the SQL Slammer worm in its tracks had system administrators properly patched their systems. Instead, the worm became one of the fastest growing Internet worms in history.

## III. TRUSTWORTHY COMPUTING

After years of criticism for releasing unstable and insecure software, Microsoft executives decided to completely retool their focus on security. They interviewed customers, technicians, and administrators to find out what was expected from Microsoft to help make networks more stable and secure. On January 15, 2002, Microsoft announced its new Trustworthy Computing initiative.

During their interviews, Microsoft heard over and over that administrators were tired of patches being released which had not been thoroughly tested, leaving their systems in worse shape than before the patch was applied. Microsoft decided to focus their efforts on testing patches thoroughly, even if it meant the release was delayed. Scott Charney, Chief Security Strategist for Microsoft, said in a report on the initiative's first year of progress something many administrators had already painfully learned over the years – "a poorly designed patch provides no security at all."

Trustworthy Computing also brought about a new group within Microsoft. With a decentralized development environment, finding updates to different software packages from Microsoft was a convoluted, incongruent process at best. The Patch Management Working Group was formed to address these issues and develop a better method of updating all software in a more unified way. These changes can be seen in some of the company's newer tools for patch management, including the Software Update Server and the Baseline Security Analyzer.

Microsoft took an unprecedented step of halting all software development for a period of two months, taking this time to train their developers how to write more secure code. The developers used this new training to completely analyze their work, searching for ways to make it better. This is referred to by Microsoft as "secure by design." Changes in the upcoming Windows Server 2003 are an example of this new way of thinking – more than 30 settings have been turned off or reduced in an effort to make the new operating system more secure.

As the second year of the initiative begins, Scott Charney promises Microsoft "will continue to focus on all four pillars of Trustworthy Computing including, in the security space, our SD3+C paradigm (secure by design, secure by default, secure in deployment, and communications)."

## IV. TYPES OF PATCHES

Microsoft routinely issues three main types of patches to their systems. Many administrators inappropriately use the terms interchangeably, however, they are viewed very differently by Microsoft. Paying attention to how Microsoft views their updates can make the process of securing a system less painful.

### Hotfixes

A hotfix is usually intended to fix critical problems for which no other solution is available. These patches generally do not undergo extensive testing. As a result, Microsoft recommends hotfixes only be applied on a system experiencing the specific problem addressed by the hotfix. Otherwise, administrators are advised to wait for the next Service Pack to be released which incorporates the hotfix.

### Security Patches

A security patch is a special hotfix which directly addresses a specific vulnerability. As part of Microsoft's Trustworthy Computing initiative, security patches are usually released quickly after new vulnerabilities are discovered. It is important to install security patches immediately on any appropriate systems.

### Service Packs

Service Packs generally contain groups of hotfixes which have been more thoroughly tested by Microsoft. They are intended to bring a particular system up to Microsoft's current code base. Service Packs are cumulative, meaning Service Pack 3 will contain all of the fixes contained in Service Packs 1 and 2, as well as any newly incorporated fixes. Microsoft recommends installing Service Packs on all intended systems in an enterprise to maintain consistency.

## V. DEVELOPING AN EFFECTIVE PATCH MANAGEMENT PLAN

There is a lot of homework which must be done when developing an effective plan for patch management. These are some considerations which should be addressed during the process:

### Inventory Your Environment

Before patching anything it is important to know what type of patches to look for. Develop a full inventory of systems, being sure to include:

- Operating System
- Current patch level
- Function of system
- Applications installed and their current patch levels
- Contact information for person responsible for system maintenance

### Educate Yourself

Become familiar with known vulnerabilities and how to correct them. Microsoft maintains a library of security alerts at http://www.microsoft.com/technet/security/current.asp.

It is also important to know about new vulnerabilities quickly. In addition to Microsoft's site, there are several sources which can help notify administrators of new vulnerabilities:

- CERT Coordination Center (http://www.cert.org)
- SANS Institute (http://www.sans.org)

## VI. PATCH MANAGEMENT PROCESS

An effective patch management process involves six basic steps:

### Analyze

Begin the process by analyzing the current environment. Determine what vulnerabilities may already exist in the environment and what patches are missing. There are several tools which can help with analysis. These tools will be explained later.

It also is important to analyze new patches as they are released. Not every patch is required on every system. A server which is not running an Internet Information Server probably does not require IIS-specific patches.

**Plan**

Once a list of vulnerable systems and their required patches is defined, it is time to plan for deployment. Have a routine downtime period scheduled for production machines, and make sure users are aware of the scheduled outage. Determine how to rollback a system in the event an applied patch has unexpected side-effects. Most recent hotfixes from Microsoft can be uninstalled via the Add/Remove Programs control panel. Service Packs from Microsoft offer the ability to backup existing files before installing, so make sure to choose this option when installing a Service Pack. And just in case something drastic occurs, ensure a working backup of the system is readily available.

**Test**

Sometimes properly testing a new patch cannot be accomplished thoroughly. Nonetheless, it is important to install a new patch on a non-production system representative of the environment to determine if there might be any unexpected side-effects. To put it bluntly, some patches are not tested thoroughly by Microsoft and can disrupt systems. Microsoft suggests installing patches to be tested on a cross-section of equipment found in the network. For Windows NT and 2000 servers, Microsoft suggests running System Stress for Windows NT and Windows 2000 1.0 for up to two weeks. A System Stress CD is included with Microsoft Developer Network CD subscriptions, but it is important to remember that it is not supported by Microsoft Technical Support.

**Deploy**

Deployment of necessary patches can be a time-consuming task. Some of the tools detailed later in this paper can assist with deployment of patches. Wherever possible, deploy patches to non-critical systems first. If a patch is going to cause an unexpected system disruption, it is better to have the disruption occur on a non-critical system than a critical one.

**Monitor**

Once patches have been deployed to their appropriate systems, monitor these systems to ensure they are functioning normally after being patches. If side-effects occur on the patched machine, determine whether a system rollback is necessary. If it is not possible to remove a patch, then it is necessary to restore the system from tape.

Make sure the issue addressed by a patch has been resolved. If not, report the situation to Microsoft. Continue monitoring all systems to ensure an inadvertent "patch-undoing" does not occur. Installing software or changing the configuration of a system sometimes can cause a patched vulnerability to return. Keep in mind Microsoft recommends reapplying all patches and Service Packs after installing software.

### Report

It is wise to retain an audit trail of system compliance as patches are applied. This allows administrators to easily show anyone who requires such information that their systems are adequately protected from known vulnerabilities. Keep a log of patches as they are installed on each system. Again, some of the tools detailed later can be used to generate compliance reports against an enterprise.

## VII. TOOLS TO MAKE THE JOB EASIER

### Determine What Is Required

Several new tools which help in the fight to keep systems up-to-date have been released in recent years. Some are significantly more extensive than others. But, as with any tool, there is no single, overall tool which fits every situation. A small environment does not necessarily need a top-of-the-line patch management tool which costs a fortune. At the same time, attempting to manage patches in a larger environment using a basic command-line tool might be asking for trouble.

Here are some items to consider when evaluating patch management tools:

- **Does the tool apply to all systems in the environment?** If 25 percent of systems in a network run Windows 98, a tool which does not address that operating system might not be the best choice.

- **What does the tool require to function?** Some patch management solutions require an agent to be installed on remote systems. Others require specific hardware or server software to function. Determine whether the environment is able to meet the requirements of a solution being considered.

- **Does the tool include a complete library of patches, and does it deliver new patches quickly?** Remember that attacks are usually at their highest immediately after a new vulnerability is announced. If a tool does not know about new patches immediately, the managed systems are at a greater risk.

- **Does the tool provide control over deployment?** Sometimes certain patches should not be delivered to certain machines, even though the patches are considered "missing." Make sure the solution is able to customize the deployment of patches to meet the environment's needs.

- **Does the tool monitor the network to ensure patches remain in place?** Periodic system checks are necessary to ensure "patch-undoing" has not occurred as a result of software installation or other routine maintenance. Ensure the solution is able to perform these checks routinely and easily to prevent vulnerabilities from reappearing.

- **Does the tool provide comprehensive reporting?** The larger an environment is, the greater the need for system reporting becomes. Tools should be able to generate routine reports on system compliance for auditing and planning purposes.

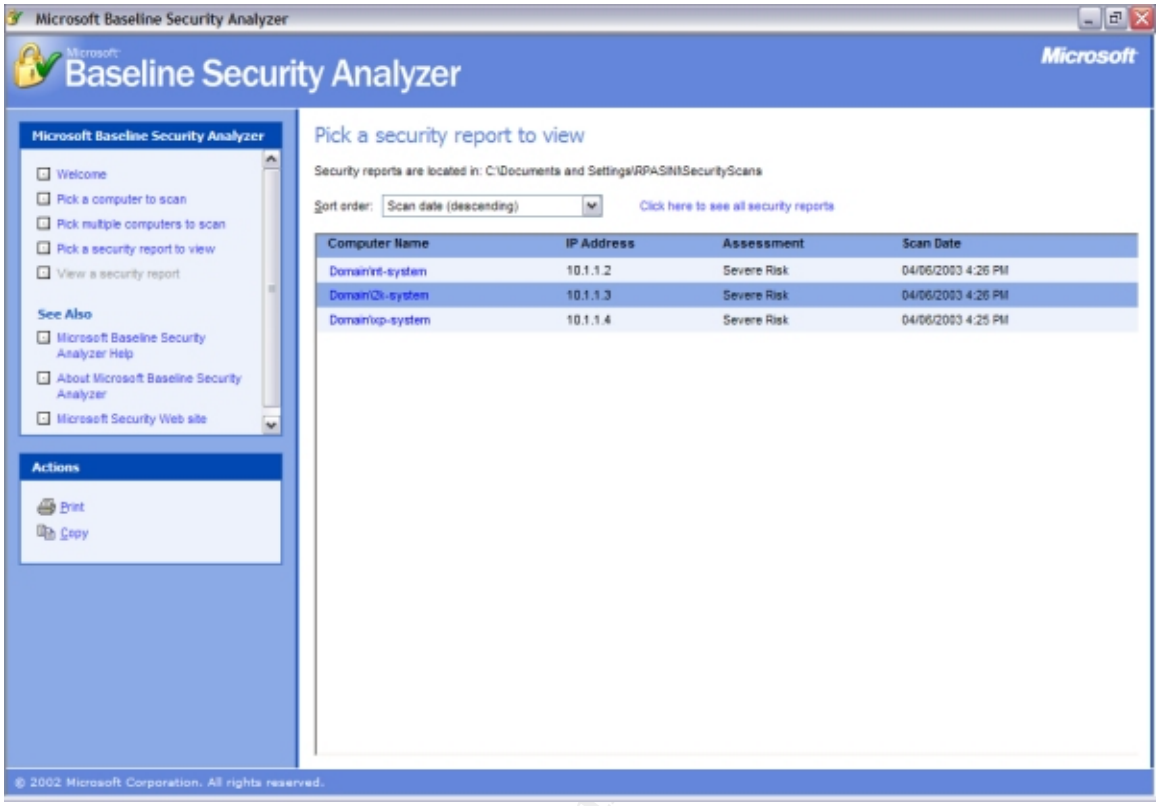
- **Does the tool scale to the environment?** Make sure the tool being evaluated fits the size of the environment. Using a tool which is not comprehensive in a large environment means most of the work will be done by hand.

## VIII. FREE TOOLS

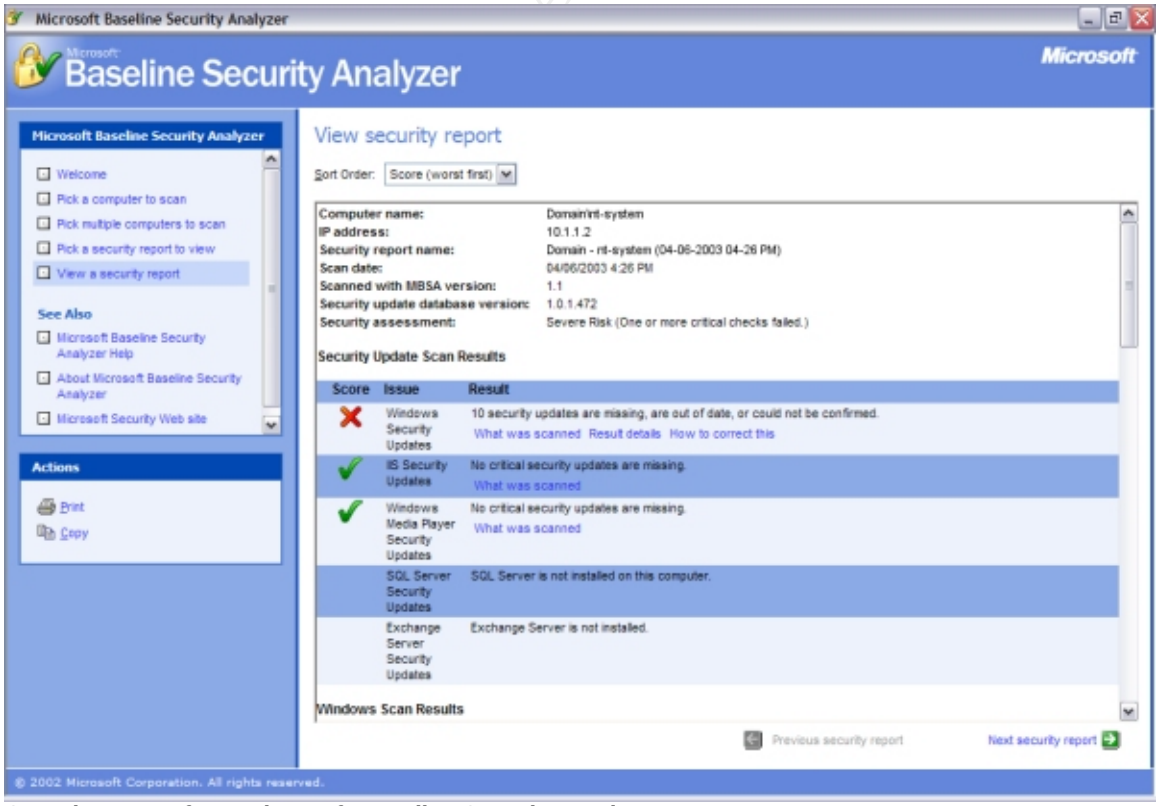
There are a number of free patch management utilities available for administrators. While they are good at simple scanning of one or several systems, most free tools tend not to offer more complex features, such as patch deployment and compliance reporting. As a result, these tools are best suited for smaller environments or spot-checks in larger environments.

### Microsoft Baseline Security Analyzer

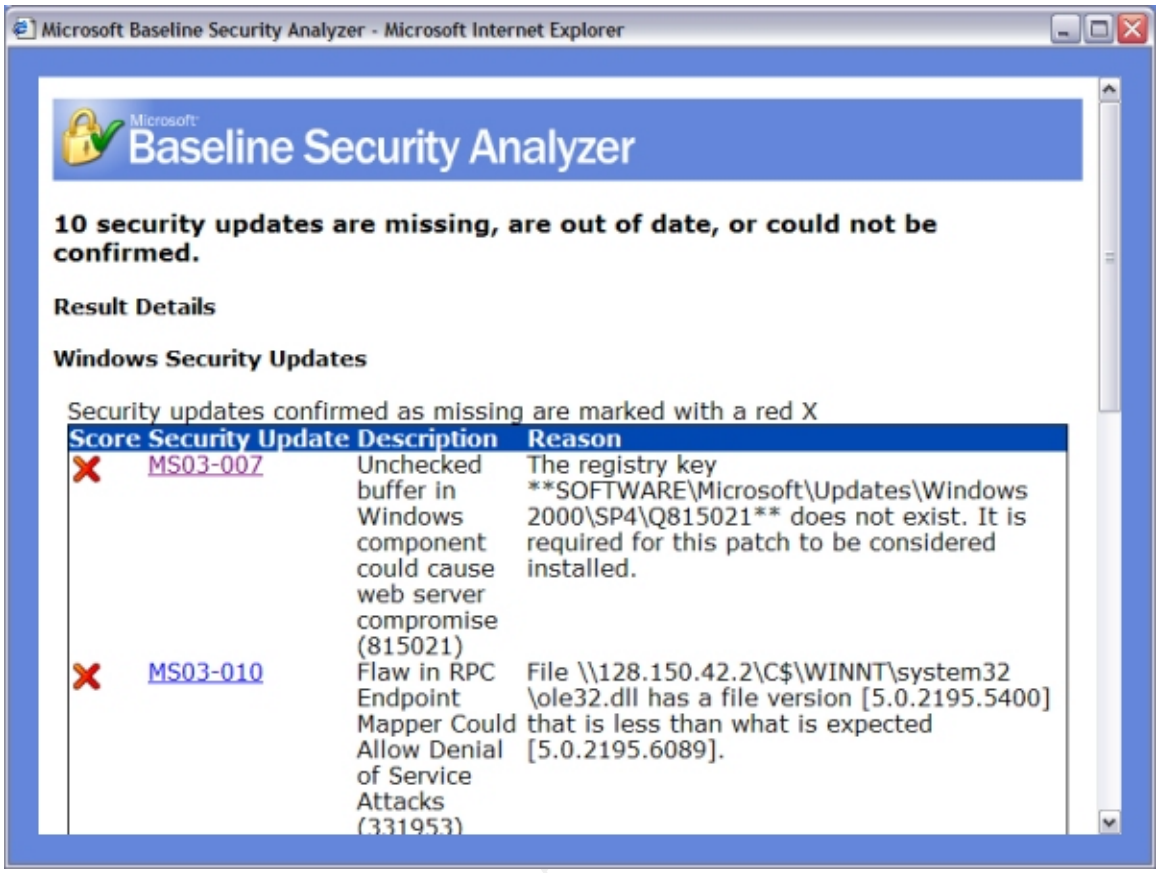
Based on HFNetChk technology licensed from Shavlik Technologies, Microsoft developed the Microsoft Baseline Security Analyzer to assist network administrators with securing their Windows systems. MBSA scans systems not only for missing patches, but also for misconfigurations which could make a system vulnerable. Scanning options are limited – while it is possible to scan a single machine, and entire domain, or a contiguous IP range, selecting which machines to scan is not possible.




***Scan results from Microsoft Baseline Security Analyzer***



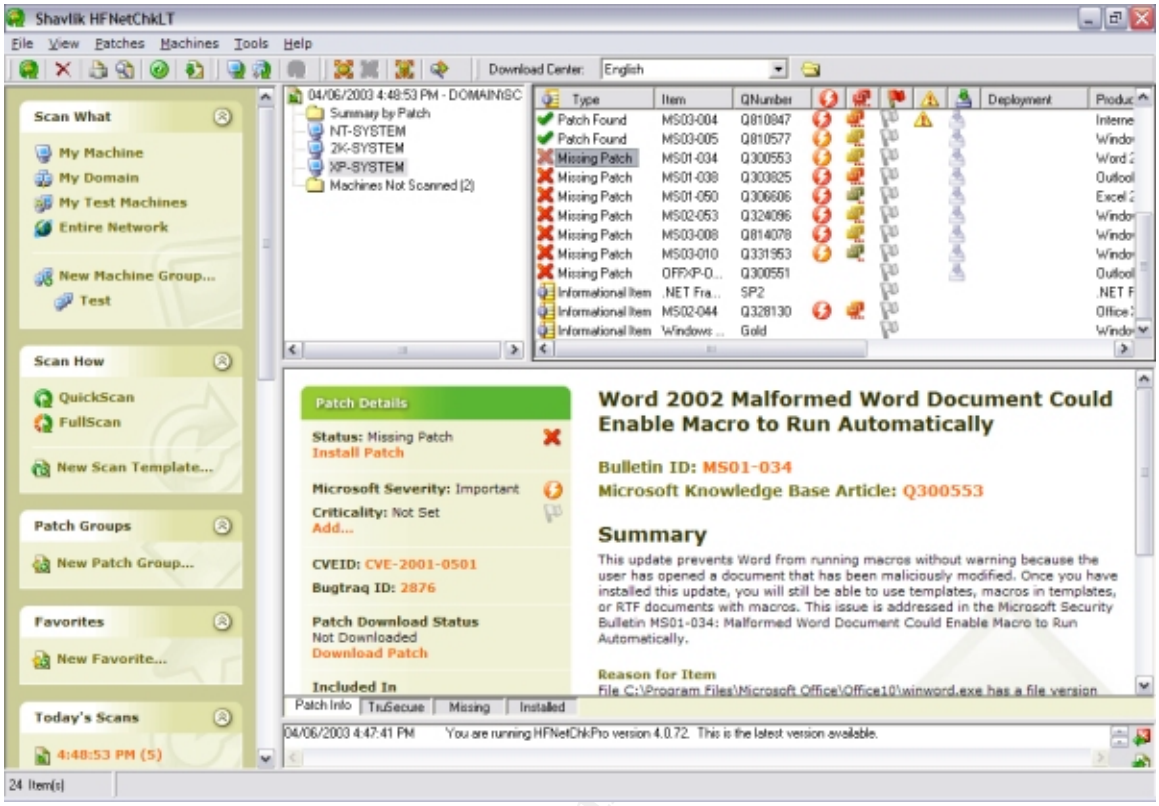

***Security report from Microsoft Baseline Security Analyzer***




***Result details of Windows System Updates in Microsoft Baseline Security Analyzer***

### Shavlik HFNetChkLT

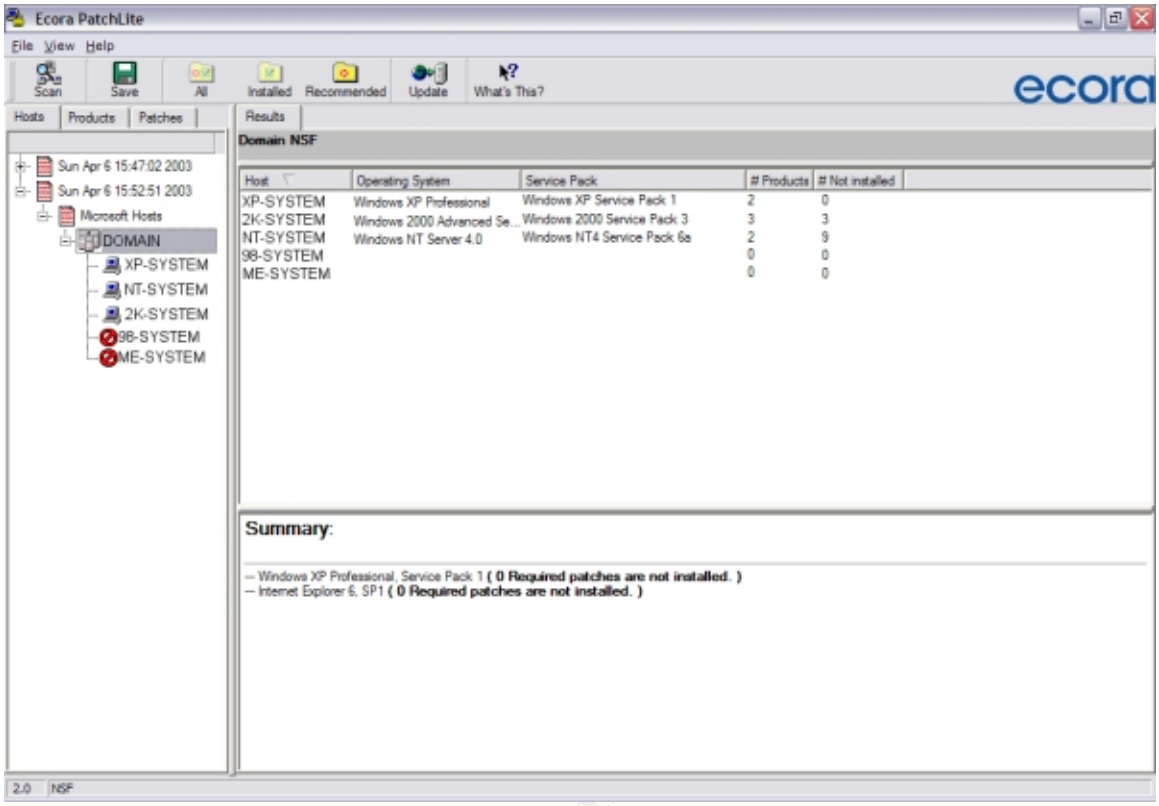
Users of the Microsoft Baseline Security Analyzer will recognize the HFNetChkLT interface, because Microsoft licensed the technology behind MBSA from Shavlik. Although HFNetChkLT does not perform the configuration scanning MBSA does, its patch management abilities outperform MBSA by leaps and bounds. HFNetChkLT is one of the few free tools which allow administrators to deploy patches to vulnerable machines automatically. There is much more granularity to defining groups of machines to scan. Patches can be marked and deployed based on chosen criticality. Administrators can even define templates to use for scanning systems. HFNetChkLT does not offer any sort of reporting capabilities; however, its major limitation is its inability to scan more than 50 systems.



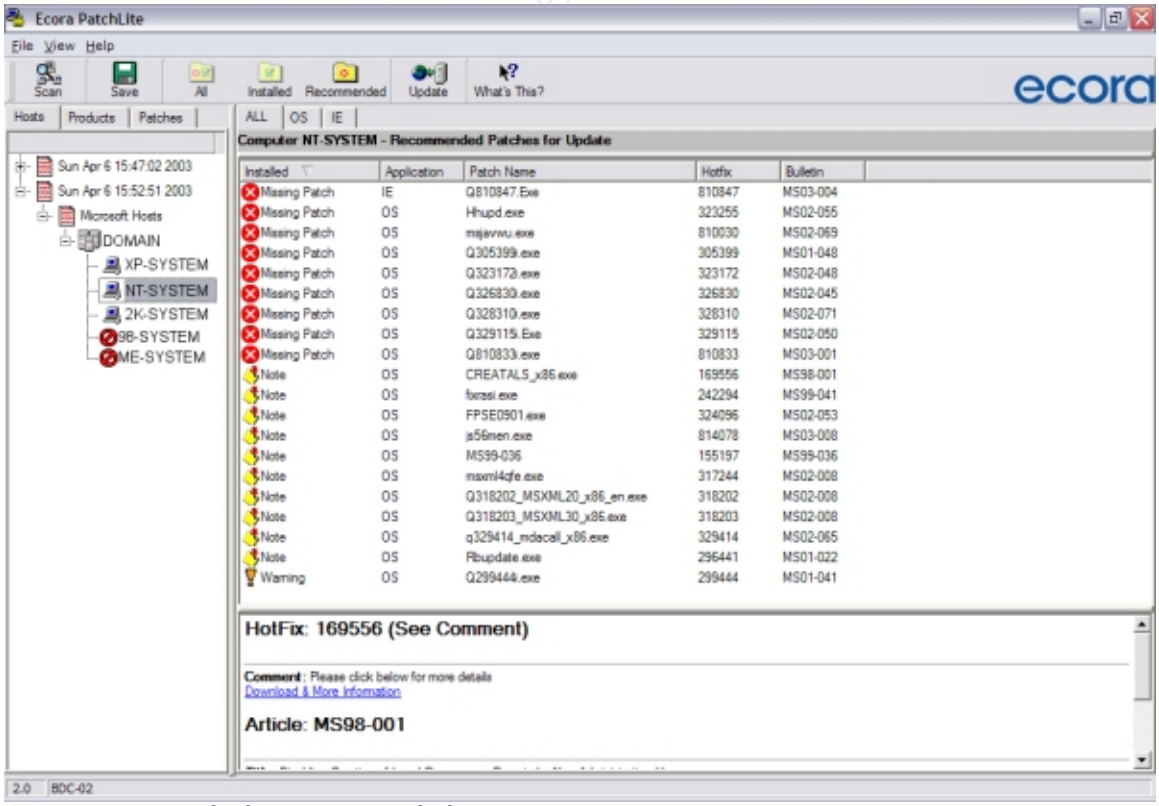

***Scan results from Shavlik's HFNetChkLT***

**Ecora PatchLite** (http://www.ecora.com)

PatchLite is a basic tool which scans a selected group of machines when requested, then display which patches are installed and which are not. As with most free tools, PatchLite lacks any type of reporting and deployment facilities. Its interface is easier to use, however, than MBSA.




***Patch management interface in Ecora's PatchLite***




***System scan results in Ecora's PatchLite***

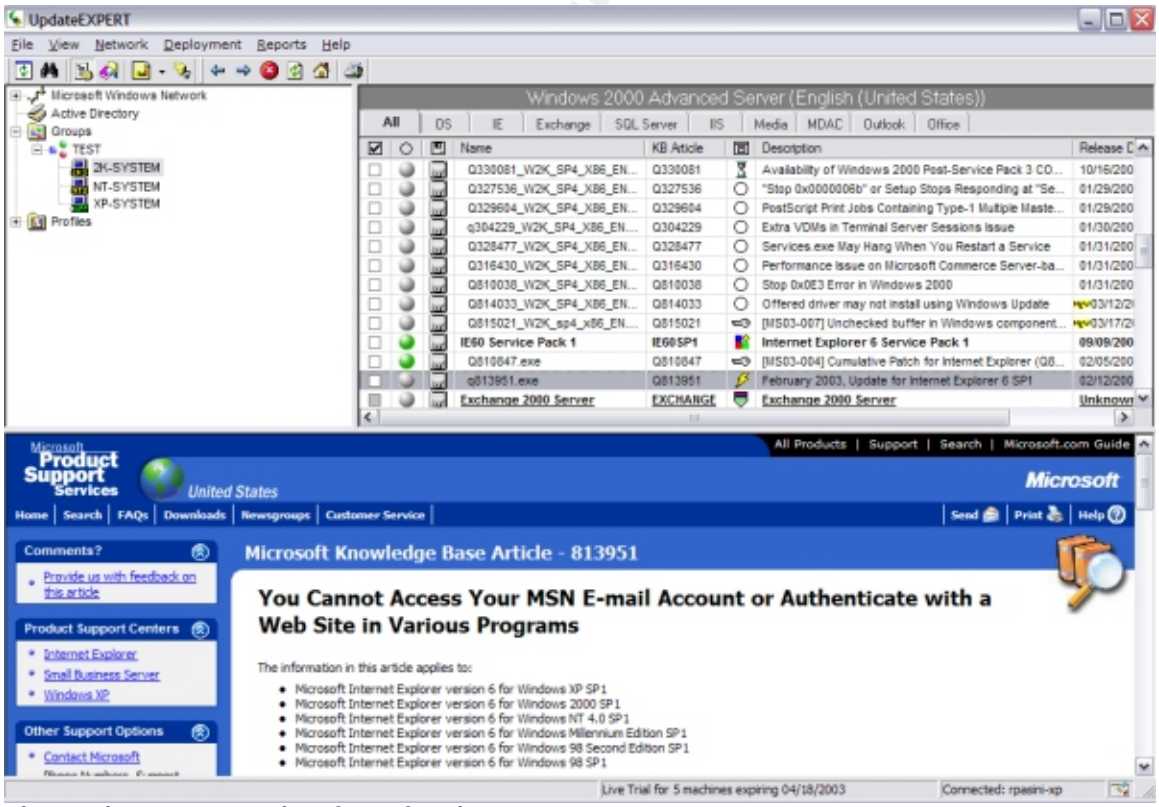
## IX. COMMERCIAL TOOLS

Commercial tools tend to offer features more suited to larger networks. These additional features generally include a method of deploying patches, reporting patch compliance, and defining the severity of a patch.

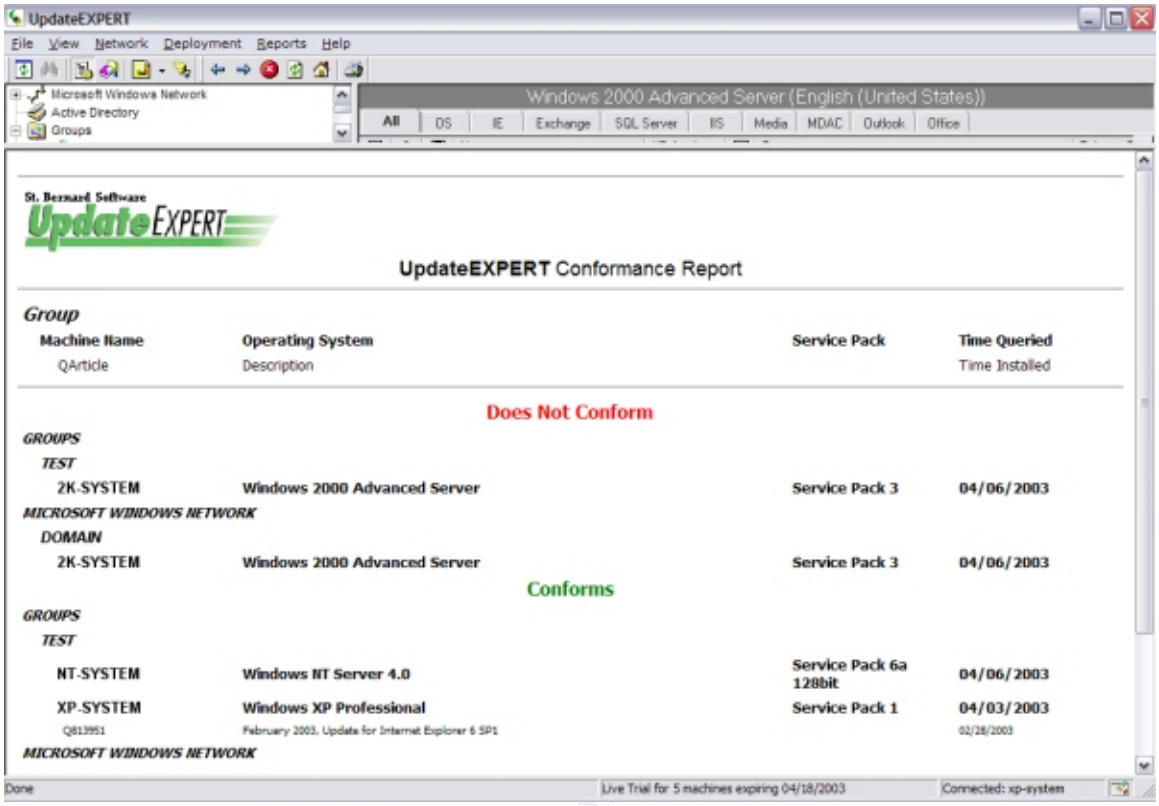
**St. Bernard UpdateEXPERT (**http://www.stbernard.com/)

UpdateEXPERT scans Windows NT, 2000, and XP systems for missing patches. Additionally, UpdateEXPERT is able to scan Windows Terminal Server machines. Like most other tools, Internet Explorer, Windows Media Player, Internet Information Server, SQL Server, Exchange, and Office also are scanned for patch compliance.

Although not required, administrators can choose to install agents to provide greater manageability of remote machines. As systems are found to be vulnerable, patches can be deployed automatically to close the vulnerability. Systems can be grouped to provide greater granularity of scanning and deployment across the enterprise. While UpdateEXPERT does offer reporting functionality, it is not as robust as other commercial tools.




***The patch management interface of UpdateEXPERT***




***Sample report from UpdateEXPERT***

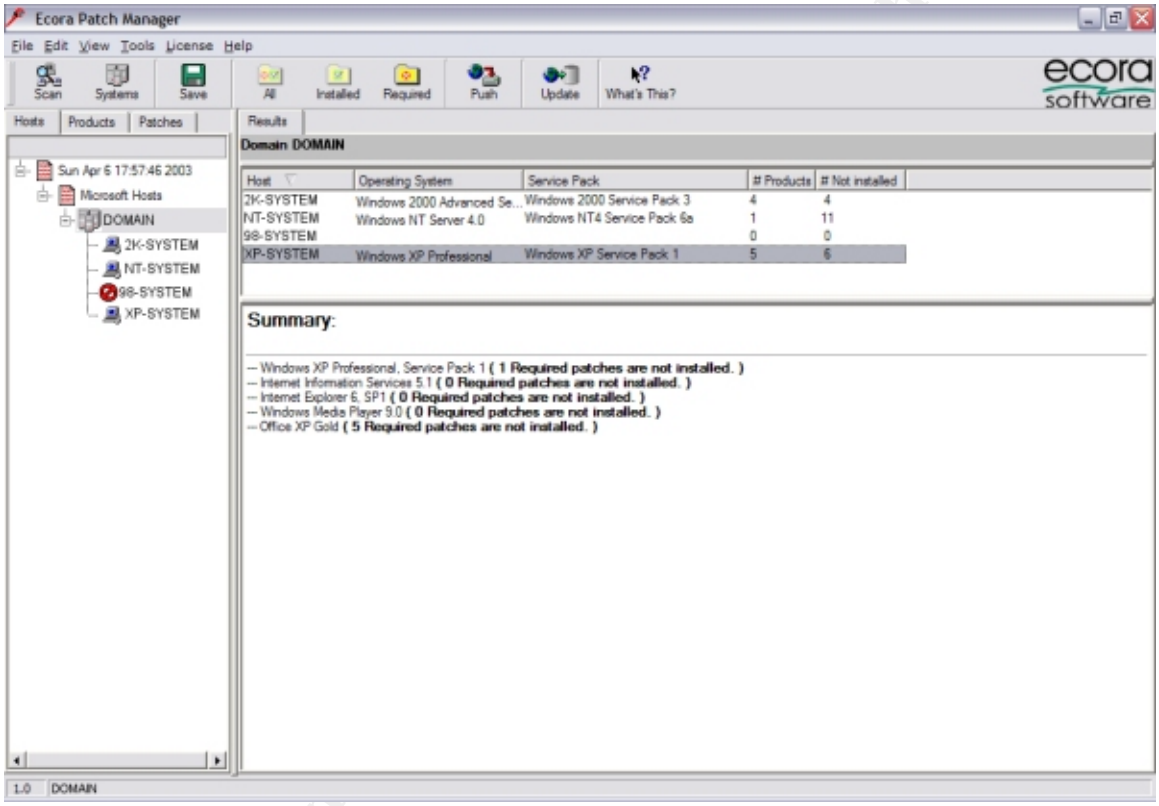
**PatchLink Update 4.0** (http://www.patchlink.com)

Again, PatchLink's Update 4.0 scans the expected operating systems and applications (NT, 2000, XP, IIS, Exchange, IE, WMP, SQL). What sets PatchLink's entry apart is its ability to scan a wide range of operating systems and applications beyond the expected, including Windows 95, Windows 98, Windows Me, and Windows .NET Server. As an added bonus, PatchLink Update can scan for patches in software from IBM, Adobe, Corel, Symantec, McAfee, Compaq, WinZip, Citrix, and Novell. As if this vast library of patches were not enough, administrators are able to develop patches to custom applications developed in-house and deploy them using PatchLink's software.

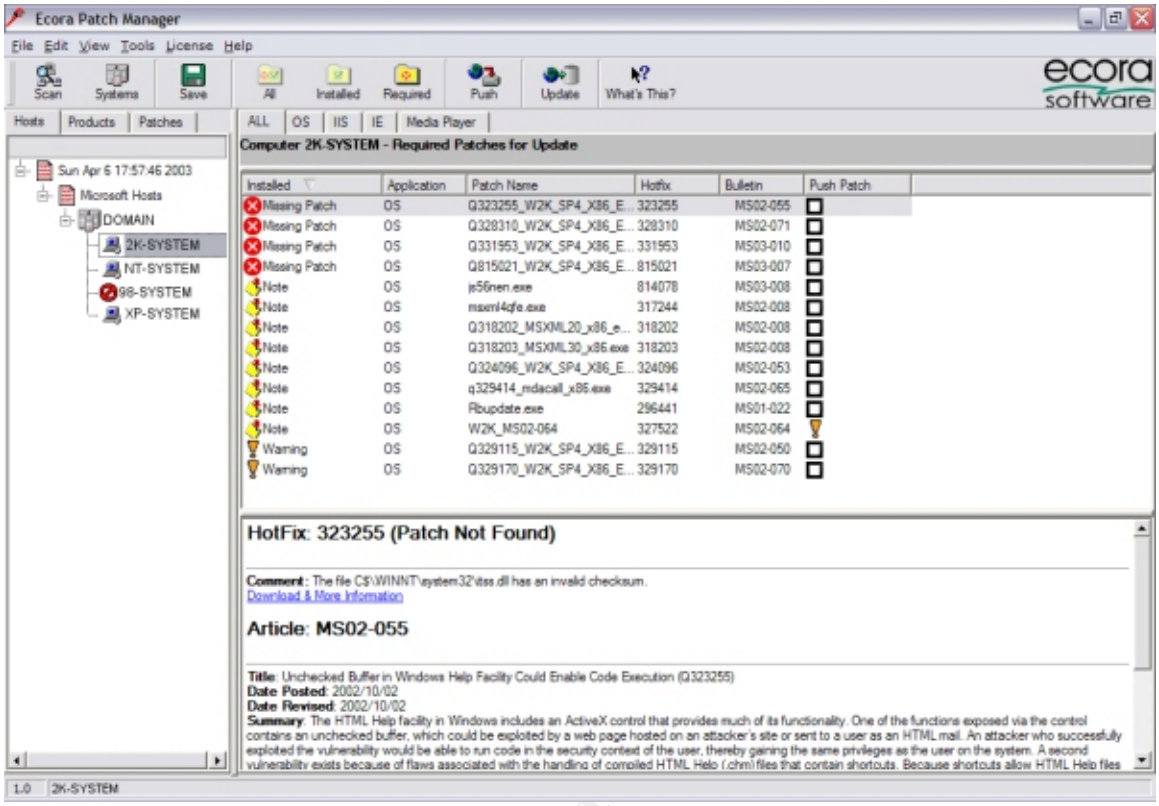
Update utilizes QCHAIN.EXE technology to chain patch installations together whenever possible, making deployment of patches faster and easier since reboots are avoided. Administrators can test the deployment of patches to system groups before actually performing the deployment. In the event a deployment causes unexpected results, Update provides the ability to rollback the entire patch deployment. PatchLink has clearly provided one of the most comprehensive patch management tools on the market.

**Ecora Patch Manager** (http://www.ecora.com)

Ecora's commercial version of their patch management tool offers a few more features than their free version. Besides scanning the basics (NT, 2000, XP, IIS, Exchange, WMP, and SQL), Patch Manager offers the ability to download the patches and deploy them to scanned machines as needed. Ecora also makes it easier for administrators to learn of new patches as they are released by alerting via email, SNMP, or event log. Since no agent is required, machines can be scanned easily without prior preparation. An HTML-based reporting facility allows administrators to audit their systems for compliance and retain the records for future review.




***Patch management interface in Ecora Patch Manager***




***Scan results in Ecora Patch Manager***

## X. CONCLUSION

As software becomes more and more complex, vulnerabilities appear all over the map. It is a race between administrators trying to patch vulnerabilities and the hackers trying to exploit them. Overlooking patch management in an enterprise can be as devastating as publishing sensitive information publicly. Microsoft has taken drastic steps with its Trustworthy Computing initiative to make their software more secure and easier to manage through better security patches, but that does not solve the entire problem. Staying on top of these patches and new vulnerabilities is a challenging task, one which is almost impossible without proper tools. While the available free tools can assist administrators with a small network, a significant investment of money and time is essential to properly protect larger environments. Only with an investment into cutting-edge technology and top-notch expertise can larger environments defend against a new breed of attacks that will continue to threaten companies into the future.

## XI. REFERENCES

"Microsoft Security and Hot Fix Bulletin Service." Microsoft Corporation. 6 Apr. 2003. <http://www.microsoft.com/technet/security/current.asp>

Collett, Stacy. "Perfect Patch Management Requires a Patchwork of Vendors." 15 Jul. 2002. ComputerWorld. 6 Apr. 2003. <http://www.computerworld.com/securitytopics/security/story/0,10801,72632,00.html>

Rosato, Rick. "Best Practices for Applying Service Packs, Hotfixes and Security Patches." Microsoft Corporation. 6 Apr. 2003. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpsp.asp>

"Microsoft Solution for Securing Windows 2000 Server." 5 Feb. 2003. Microsoft Corporation. 6 Apr. 2003. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp>

"The Journey to Trustworthy Computing: Microsoft Execs Report First-Year Progress". 15 Jan. 2003. Microsoft Corporation. 7 Apr. 2003. <http://www.microsoft.com/presspass/features/2003/Jan03/01-15twcanniversary.asp>

Mueller, Patrick. "PatchLink Helps Keep Windows Closed." Network Computing. September 2002. TechWeb. 6 Apr. 2003. <http://www.networkcomputing.com/1318/1318f3.html>

"Security Patch Management: Antidote to Network Vulnerabilities." Big Fix, Inc. 6 Apr. 2003. <http://www.bigfix.com/website/enterprise/download/Patch_Management_White_Paper.pdf>

"Patch Management: Get on Top of IT." Security Post Issue 3. 6 Apr. 2003. <http://www.dnsltd.com/securitypost/issue3.pdf>

Mullen, Tim. "Patch Management Done Right." 6 May 2002. Security Focus. 6 Apr. 2003. <http://www.securityfocus.com/columnists/79>

DeBellis, Matthew A. "Patch Management Software IT Pro's Friend." SearchWindowsManageability.com. 29 Oct. 2002. TechTarget Network. 6 Apr. 2003. <http://searchwindowsmanageability.techtarget.com/originalContent/0,289142,sid33_gci860091,00.html>

Wilcox, Joe. "Microsoft Server Share Jumps in 2001." News.com. 23 Sep. 2002. CNET. 6 Apr. 2003. <http://news.com.com/2100-1001-959049.html>

"CERT/CC Statistics 1988-2002." CERT Coordination Center. 6 Apr. 2003. <http://www.cert.org/stats/cert_stats.html>

"Internet Domain Survey, January 2003." Internet Software Consortium. 6 Apr. 2003. <http://www.isc.org/ds/WWW-200301/index.html>

"NUA Internet – How Many Online?" Scope Communications Group. 6 Apr. 2003. <http://www.nua.ie/surveys/how_many_online/index.html>

Hubley, Mary and Mary Ann Richardson. "Service Pack Management for Windows Operating Systems: Perspective." Gartner Group Technology Overview DPRO-90911. 24 Apr. 2002.

Nicolett, M. and J. Pescatore. "'SQL Slammer' Lesson: Patch Management Is Not Enough." Gartner Group Research Note T-19-3534. 13 Feb. 2003.

Nicolett, M. and R. Colville. "Robust Patch Management Requires Specific Capabilities." Gartner Group Research Note T-19-4570. 18 Mar. 2003.

Brykczynski, Bill and Bob Small. "Improving The Security Patch Management Process." June 2002. Software Productivity Consortium.

Colville, R. and M. Nicolett. "Patch Management: Identifying the Vendor Landscape." Gartner Group Research Note M-19-4562. 18 Mar. 2003.