Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Home Computer Security Patch Options For Corporate Security Managers.

For the purposes of this paper, I'm interested in people who use their home computers to connect to a corporate LAN via a Virtual Private Network (VPN) tunnel over a residential broadband Internet connection. The principles discussed will apply to any remotely connected user allowed to access protected systems behind a firewall, but to keep the paper concise we'll focus on residential home-based VPN users. Users connecting through dial-up modems are being excluded from this paper because the bandwidth available to them...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.
watchfire

HOME COMPUTER SECURITY PATCH OPTIONS FOR CORPORATE SECURITY MANAGERS.

Timothy Rice
July 3, 2003
V1.4b

ABSTRACT

For the purposes of this paper, I'm interested in people who use their home computers to connect to a corporate LAN via a Virtual Private Network (VPN) tunnel over a residential broadband Internet connection. The principles discussed will apply to any remotely connected user allowed to access protected systems behind a firewall, but to keep the paper concise we'll focus on residential home-based VPN users. Users connecting through dial-up modems are being excluded from this paper because the bandwidth available to them while connected make remote patching impractical. Furthermore, reduction in available dialup bandwidth would seriously hamper users' ability to perform any of their intended tasks.

As corporate Internet connections become more secure over time, the need for remote users to access network resources will not change. A mobile sales force needs access to the latest up-to-date product numbers and information, an on-call physician still needs access to confidential patient records, lawyers continue to need access to client documents. This need to access secured network resources is the driving force behind the increasing use of VPN's. Purchasing, installing, and configuring an expensive VPN router is not enough. You must take steps to ensure defense in depth at *both* ends of the connection. If the remote systems are not properly secured prior to the tunnel being created, the entire LAN is potentially unsecured. All of the systems we will examine were originally intended to manage patches for either stand-alone consumer systems or a centrally managed LAN. What we will consider is what features will allow them to manage systems that occasionally become local due to a VPN connection.

THE PROBLEM

In May of 2003, Sophos released a report indicating that upwards of 70% of network administrators are only updating anti-virus information on a weekly basis for remote systems[1]. Since applying security patches is even more complicated and time consuming, it is safe to assume that they are applying these patches to the remote systems even less frequently. With the continuing growth in use of Virtual Private Networks (VPN's) to access corporate information systems[2], this is a troubling condition. Any system that connects through a VPN needs to be maintained just as rigorously as the local systems since from the perspective of the network it is local once the VPN connection is established. Any baggage a remote system is carrying in terms of Virus infections, Trojans, or other types of Malware come into the LAN when the VPN tunnel is created.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Traditionally, home computers are the most poorly supported systems connected to the Internet. This is a fact that hackers and virus writers routinely exploit. Thanks to the tireless hard work of software vendors, computer makers, and broadband ISP's everywhere; anyone can buy a computer, take it out of the box and connect it to the Internet via a high speed, "always on" broadband connection with very little effort. If the home computer becomes infected with the latest Trojan or other malware, and the computer is then used as an end point for a VPN tunnel, the protected zone inside the corporate network is exposed to the threat of the malware. Any resources accessible by the user are now available to the Trojan and the expensive firewall is potentially rendered useless. Keeping the home systems properly patched will help minimize the chances of this happening.

The task of keeping Windows based computers properly patched and secured is a full time, often confusing job for a professional support staff. A quick perusal of the SANS.org Reading Room will quickly convey this impression. Imagine how confusing it is for an average end-user. The average home user can follow the directions provided by the PC makers and the ISP such that they could connect a computer to the Internet at home with little or no assistance. It is doubtful that they would be nearly as successful making it secure and keeping it that way over time and given their inevitable lapses in good judgement.

When a corporation is encouraging or requiring users to access LAN resources remotely via a VPN, it must make a reasonable effort to ensure that the computers accessing the VPN are properly patched, secured, and remain that way, both for their own sake, and for the sake of the Internet as a whole. All home systems should be running some form of Personal Firewall, and for added protection, need to be situated behind a modern Small Office, Home Office (SOHO) router that provides Network Address Translation (NAT)[3]. In addition, in accordance with established Best Practices, all applicable security patches should be applied in a timely manner[4]. The corporation should also supply licensed Anti-Virus software and keep its definition files current.

Legal and User Acceptance Issues

There can be no doubt that there are potential legal issues involved in deploying patches to home based systems. If the computer to be patched is not the property of the corporation, what happens when a patch goes bad and the system crashes? Was the users spouse using the system to operate a home-based business? Did it have the user's tax returns on it? Is the data recoverable, who recovers it?

The coverage of the legal issues is not within the scope of this paper, but it is definitely a subject that needs to be carefully addressed by management prior to initiating any patching system.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The establishment and communication of a Corporate VPN policy[5] can mitigate some of the issues. The policy needs to clearly state that any system connected to the corporate network via the VPN must be kept properly patched in an auditable manner, and that as such, the corporate patch management system must be applied to the computer. The Policy should spell out who is responsible for any problems resulting from the patching process, and what remediation is available in the event of a patching related problem.

Timely and efficient communication with users is a key element in any patch management system. It is even more important when addressing home systems. Notifying users prior to distributing a patch or allowing users to defer patches can instill a sense of control and ownership in the process. While fully explaining what is about to happen is important, it is just as important to explain *why* it is happening. The average user has no idea that their systems are vulnerable to attack, and if it is explained that the patching is done to protect them along with the corporation, they are more likely to accept the system and not become an impediment.

Technical hurdles to a remote patching system

Connection

The first hurdle that needs addressing in any home computer patching system is hopefully the inability to contact the remote computers directly. These remote systems are all supposed to be safely located behind a SOHO router and a personal firewall.

The fact that home systems are turned on and off at odd times will complicate the problem of establishing contact from the LAN. With systems physically connected to the corporate LAN, there is a good chance that between the hours of 8am and 5pm they will be turned on and performing tasks. In some cases, corporate users on the LAN are not even granted the rights to shutdown their workstation. The complete reverse is usually the case for home systems.
A third impediment to patching home computers is the extremely wide range of possible hardware and software in use. Local systems purchased by an organization typically adhere to some form of standards in terms of both the hardware and the software being used.

One way to avoid having to patch a random collection of hardware, software and Operating Systems is for the corporation to make the decision to purchase systems for employees to use for accessing the LAN, and performing work related functions. Stipulations can be made that the computer is still the property of the corporation and that it is intended for work related tasks. This will not prevent spouses and children from using the computer for other tasks, but it should help with potential legal issues and will provide a much more homogenous environment to be patched.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Size and frequency of software patches

Patch distribution can be a bandwidth intensive activity, and usually needs to occur on a regular basis so care needs to be taken in choosing a solution for home systems. In 2002, Microsoft released 72 different patches for the Windows family of operating systems. That works out to about one patch every 5 days. Service Pack 4 for Windows 2000 was recently released and weighs in at 129MB. Even with a broadband connection, that's a large download.

Patch Distribution

Since home systems are not always connected through the VPN, the question of where to place the patch distribution points comes up. Do you place the patch management system entirely behind the corporate firewall, or do you expose portions of it to the Internet? This decision will be heavily influenced by the abilities and security features of the patching system used.

If we choose to place the system entirely within the organizations LAN, then the home systems can only access it while actively connected via the VPN. This will limit the number of home systems that can be patched at a time since VPN routers are usually limited in terms of the number of simultaneous connections they can effectively support. Too many simultaneous users is likely to slow the VPN router, and further exacerbate any bandwidth issues. The more restricted the bandwidth, obviously the longer it takes to transfer the files, and the greater the risk of the connection being broken by the user. The ability to resume an interrupted download can make or break such a system.

One way to avoid choking the VPN server is to download the security patches directly from Microsoft. There is a slight risk in this since Microsoft has been known to update patches, and you could wind up with the patch being replaced midway through the deployment process. Any system that attempts this should have the ability to verify the patch with some form of checksum.

The other choice is to expose a portion of the patch management system to the Internet, thus allowing the home system to retrieve patches at any time. Extreme care must be taken to secure and harden the OS of the exposed server. It would be tragic if the patching system was used to compromise the systems.

Bandwidth management

Anyone who has ever used a VPN knows that a VPN induces overhead in terms of available bandwidth and available processor cycles. The exact impact of the overhead is difficult to estimate since it is highly dependent on the encryption methods used, the processing power of the VPN router as well as the remote system. The speed of the connection also plays a part in determining overhead. Downloading patches will further exacerbate the perceived overhead. Some patch management systems allow the download of the patch to be limited or throttled and also allow it to be restarted if the connection is lost in the middle of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the download. These are traits to look for in any solution. Windows 2000 Service Pack 4 is a 129MB download. Even using all of the available bandwidth on a good Cable or DSL connection, downloading 129MB is a time consuming process. Without the ability to throttle or limit the download speed of the patch, the user will likely be unable to perform the tasks for which they originally created the VPN tunnel. If the solution does allow throttling of the download, then it will by definition extend the time required to download the patch, and increase the risk that the user will tear down the tunnel before the download is completed. This highlights the need to seamlessly resume interrupted downloads.

People communication / user interaction

End user communication is an effective way to help deal with the dilemma of large downloads. If the users understand the need for the patches, and are given advanced warning, they may accept the download as a necessary activity. There will always be users that for various reasons cannot or will not accept the patches when scheduled. Giving them the ability to defer or delay the patch download and application might improve overall compliance.

DESIREABLE FEATURES

To accomplish the task of auditing home computers and deploying patches to them in a reasonable manner, with minimal impact on the user, there are some features that an effective solution should have.

Agent-based.

Patch distribution software comes in one of two flavors: Agent-based and Agentless. The agentless systems rely on the ability of a management console to contact the target system using Windows RPC protocols. To be effective, the target system must be turned on and accessible at the time the scan is run. Another drawback of agentless systems is the large volume of network traffic generated during the scan process.

Agent-based packages operate by installing a small piece of code on the target system. This software usually runs as a Windows service and 'wakes up' on a regular basis to inspect the computer. The agents typically run at the System level to allow full control of the operating system. Once the agent has inspected the computer, it tries to contact a central server. If the server is not available, as when the VPN is not in use, it will hold the results and try again later. When contact is made, as when the VPN is active, only the changes need to be transmitted to the server thus reducing the bandwidth used each cycle.

It should be impossible to contact the home systems from inside the LAN without the VPN being active so agent-based systems are the only viable answer. Agent-based systems also provide the benefit of allowing a more interactive user experience. The user can delay the patching process and potentially have control over the reboot process.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Internet Protocols.

We are going to be transmitting the patches over the Internet so it only makes sense to use standard Internet protocols to do so. Since access to the corporation's central Windows shares is restricted to local clients, and a remote system cannot access them unless it is actually running the VPN client at the time, we should focus on packages that offer other ways to download patches. Standard Internet Protocols such as HTTP and FTP are the best choices. Since these protocols are designed for the Internet, there should not be any special hardening or server configuration required beyond those normally required by the average Internet server.

Pull based patch distribution.

Once it is determined which patches a computer needs, there are two ways to deliver the patch. Push and Pull. With the push method, the Windows RPC protocols are once again used to 'push' the patch from a central point out to the remote systems. Pull based distribution works by having the remote system initiate and manage the transmission of the patch. Agent based systems tend to use a pull method for distribution, it allows them to better manage the process.

Ability to throttle bandwidth use.

Since home users usually have limited bandwidth available, it would be beneficial to the users overall experience if we could limit the amount of available bandwidth that the patch transmission uses. It will extend the time it takes to distribute and apply a patch, but since it will impact the users much less it should result in reduced negative feed back from users, and greater acceptance of the system. The only way to throttle the transmission is to use an Agent based pull method. The native Windows file transfers and PRC protocols don't include any mechanisms that can throttle the transmission.

Ability to resume interrupted downloads.

Hand in hand with the ability to throttle a transfer is the ability to resume an interrupted transfer. Since a throttled transfer will take longer to complete, the chance of it being interrupted either by the tunnel being torn down or the system being shutdown is greater. Having the ability to resume an interrupted transfer will greatly decrease the number of attempts needed to actually complete a patch transfer, and thus decrease the overall time required to complete the application of a patch. Both agent based systems and agentless systems affect the transfer of files without the user having to be directly aware of the process. In most cases the user will not be notified prior to the transfer, and will also not be notified when it is complete. As the patches get larger, so does the chance that it will be inadvertently interrupted by the user. Since we must assume that home users do not leave their computers running all the time, nor do they constantly have a VPN connection open, we need to be able to resume, rather than restart, an interrupted download.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Security.

The patch system should be secure at all steps of the process. It should not be feasible for an attacker to either inject a rogue patch into the system or interfere with current patching jobs. The potential for disaster is obvious. Since we are looking for systems that use standard Internet protocols, the use of either SSL or digital signing signatures should be a priority. Security should be a priority from the initial vulnerability reporting process, through the patch authorization, and include the patch transmission stages as well. Any point at which unauthorized information can be injected should be secured and verified.

Free solutions for Patching

Microsoft Software Update Services (SUS)[6]

Microsoft's SUS with SP1 is a good solution for keeping home or remote systems reasonably patched at minimal expense. The following server requirements from Microsoft are designed to support upwards of 15,000 clients so if your client base is smaller, you should be able to reduce the server requirements. That said, it's a good idea to stick with the recommended minimums where possible

Server Requirements

- Pentium III 700-mhz
- 512MB RAM
- Network Connection
- NTFS partition with 100MB free to install system
- NTFS partition with 6Gig free if Administrator chooses to store and distribute patches from SUS server
- IE 5.5 or later
- Microsoft Internet Information Server (IIS)

Client Requirements

- Windows 2000 Service Pack 2
- Windows XP
- Windows NT4 and earlier OS's are NOT supported.

SUS can deploy the following types of patches

- Windows Critical Updates
- Windows Critical Security Updates
- Windows Security Roll-ups

SUS will not deploy Service Packs, drivers or patches for any other types of applications such as SQL Server, Exchange Server, or the Office suite. It is also not possible to deploy custom written patches. The lack of ability to deploy SQL Server and Exchange Server patches should not be an issue with home based computers.

The only financial costs directly associated with SUS are for the server hardware, OS licenses, and labor on the part of the Administrators. With the recent release of SUS SP 1, the server software can be installed on a Domain Controller or a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Small Business server although Microsoft does not recommend this. Depending on the number of clients to be supported, it might be better to house it on standalone hardware. There is also the question of where to locate it in the network topology.

With the client set to run in Automatic mode, end users do not require Local Administrator rights on their computers. They are presented with a warning 5 minutes before the patches begin to apply. The updated client can now be configured to not force a reboot if there is a user currently logged into the computer at the time the patch is applied. The user is presented with a dialog box allowing them to cancel the reboot or allow it to proceed. The client also obeys any policy settings regarding the user's ability to restart the computer. If a non-Administrator user without reboot rights is logged onto the computer when a patch is applied, the system will notify them that a patch has been applied, then wait until they have logged off the computer to reboot it. This is done to prevent user data loss.

If a computer misses a scheduled update because it was turned off, it will attempt to retry the update when it is next turned on. If a Reschedule Wait Time is defined, then once the update service is started, it will wait the defined number of minutes before starting the update. The setting can be between 1 and 60 minutes.

Microsoft WindowsUpdate WWW site

Microsoft, in an attempt to make security patches more accessible, created their WindowsUpdate WWW site. WindowsUpdate is an ActiveX driven WWW site that will scan your computer to determine which patches are missing, then present a comprehensive list of necessary and recommended patches organized by the type of patch.

The WindowsUpdate site is targeted primarily at consumers, and is very simple to use. It does require that the user have Local Administrator rights on the machine being patched but this is not likely to be a major impediment for home users. There are papers in the SANS.org Reading Room that address WindowsUpdate[7].

Windows 2000 SP2 included the Automatic Update service. This small service monitors the Windows Update WWW site and depending on how it is configured, will pre-download the patches needed and prompt the user when they are ready to be applied.

One benefit of the WindowsUpdate site and the Automatic Update service is that the patches come directly from Microsoft. Whether or not the user is running the VPN at the time or not, the patches can be applied.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

For security, Microsoft digitally signs all their patches. Authenticity of all patches is verified prior to actual installation.

The primary drawback to using WindowsUpdate is the lack of any reporting capability. Since everything is performed at the remote workstation, and no remote reporting functions are provided, an Administrator has no way to track the patch status of the remote systems they are responsible for.

BigFix Consumer Version[8]

Another free solution available for patching home computers comes from BigFix, Inc.. The Consumer version of their software uses the same Fixlet technology that their BigFix Enterprise Suite uses, but is delivered through a stripped down client. The consumer version checks for new fixlet messages on a scheduled basis. There are several 'sites' that can be subscribed to. The choices include sites for Win95, Win98, WinME, WinNT, Win2k, and WinXP.

Minimum Requirements include a Pentium processor, 32MB of RAM and at least IE 4. All versions of Windows from Win95 through Windows Server 2003 are supported.

The consumer version of BigFix is not an automated tool. It does notify the user through a system tray icon that patches are available. BigFix will apply all service packs and includes patches for Office products if installed on the computer.

To apply most OS level patches, the active user would need to have Local Administrator rights on the computer to be patched.

Because it lacks automation of the patch application process, lacks reporting capacity, and requires Local Administrator rights on the computer, BigFix Consumer version doesn't provide any additional functionality over and above the WindowsUpdate WWW site. The only benefit might be for people with privacy concerns regarding WindowsUpdate services.

Privacy issues not withstanding, the ability to automate WindowsUpdate through the Automatic Update service included in Windows 2000 SP2 makes it a superior product for maintaining the patch levels on operating systems still supported by Microsoft. If there is a need to maintain patches on operating systems for which Microsoft is no longer providing support, BigFix Consumer version is an excellent choice.

Commercial Solutions for Patching

Without trying to cover every commercial automated patch management system, we'll look briefly at several examples. The criterion used here can be applied to any patch management system.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

BigFix 3.0[9]

BigFix 3.0 is an Agent based system and uses the http protocol for it's communications. When the server is installed, the port can be changed if the Administrator so desires.

The client agent can throttle patch downloads, and can resume a download at a later date if it is interrupted. Different clients can have their bandwidth throttling set to different levels, so home systems can have a tighter throttle setting than local clients.

BigFix uses public/private key signing to secure all aspects of the patching process. All actions are signed, as are all communication between the agents and the server. The signing keys can be as small as 128bit and as large as 4096bit.

When a patch is scheduled for deployment, the administrator has the option to allow the user to Cancel the patch. A canceled patch reports back as failed, and the system will continue to show that the patch is required. If the user continually refuses to allow the patch to deploy, the Administrator can force the patch to install, and force a reboot afterward if necessary.

If the agent tries to contact the server, and fails, it will wait and try again later. BigFix refers to the period between updates as the heartbeat. If the agent detects a change in the IP address table, it will attempt to contact the server. A change in the IP table occurs when a system establishes a VPN tunnel. This would trigger the agent to attempt to contact the server to deliver it's updates and retrieve any scheduled patches.

Before a patch is distributed to a client, it is cached on the BigFix server to ensure that all clients receive the same patch. BigFix also incorporates the ability to spread the patch distribution load through the use of Relays. A Relay is a BigFix agent that has been flagged by the administrator to act as a trusted distribution point. Other agents are configured to use that agent as a Relay. If a Relay is unavailable, either because it is too busy serving other clients or is off line, the requesting agent will failover either to a secondary Relay, the central server, or to the original source for the patch. In many cases, this is Microsoft so the patches are available over the Internet. A relay server can be placed in the DMZ to allow home machines to continue to update after their VPN tunnel has been shutdown.

Patches are transferred using either HTTP or Anonymous FTP depending on how the relevant fixlet message is written.

All patches are tested internally by BigFix staff prior to being release to customers. During the patch testing, BigFix examines the contents of the patch

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

to determine which files are updated. This information is used to determine the patch's relevance to a computer.

All versions of Windows are supported. LINUX and MacOS X clients are available although there are no patches available at this time.

By default, the number of reboots required is kept to a minimum by automatic chaining of patches.

PatchLink 4[10]

PatchLink is an agent-based system that can deploy patches to all versions of Windows plus UNIX and Netware machines.

The agent has the ability to resume interrupted transfers, and automatically throttles the download.

Patches transfer to the client machines via the standard SSL protocol and the agent will throttle the communications by default. If the transfer is interrupted, it will automatically resume when it is able to.

When a patch is scheduled for distribution, the PatchLink server downloads it and stores it locally. It then distributes it to the clients. This ensures that all clients receive the same patch even if Microsoft makes an unannounced change to the patch.

Client reboots are minimized because PatchLink automatically chains all the patches.

It is possible to use a hardened WWW server to distribute the patches from a DMZ. Placing a server with a hardened OS in the DMZ would allow home systems to download their patches even when the VPN tunnel was not active. This would shorten the time required to distribute a given patch.

Microsoft SMS 2.0 with SUS Feature Pack[11]

Microsoft's flagship system management product is also capable of deploying patches. Historically what it lacked was the ability to detect which patches were needed on a computer. The SUS Feature Pack fills this feature gap.

Microsoft recommends that SMS with the SUS Feature Pack be used to deploy patches in an enterprise setting. SMS is a very mature, feature rich product. Using SMS to deploy patches in a LAN setting works well though there are several problems with extending it to patch home systems

Chief among the drawbacks of SMS is that it uses Windows Shares and Windows Authentication to deploy packages. The only time that a home computer will have access to the shares is when the VPN client is actually

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

running and it would have to have proper credentials to access the share unless it was an anonymous share.

Because SMS relies on Windows file sharing to distribute files, it is unable to throttle package downloads. It is also unable to resume an interrupted download, and would have to try the entire download the next time the user connected to the VPN.

SMS 2.0 does not support operating systems prior to Windows NT. If the corporation is purchasing systems for users this is not a problem, but trying to retrofit it to existing home users might be problematic in light of the popularity of the Win9x OS's with home users.

In the documentation for the SUS Feature Pack, Microsoft recommends that if you do not already have SMS deployed, or do not currently plan to deploy it, don't do it just to deploy patches. They recommend their stand-alone SUS product. The reason behind this recommendation is that SMS is an extremely complex system. SMS requires extensive planning and training on the part of the corporation prior to it's deployment.

UpdateExpert[12]

Version 6.0 adds new 'leaf agent' technology to improve performance and increase range of networks that it will operate in. The value of this agent to home based systems is limited since it only performs the reporting functions, and not the data transfer operations.

UpdateExpert uses Push technology, so remote systems must be connected to the network, and the system that initiates the push must have valid credentials on all the remote computers. This fact makes it difficult to deploy UpdateExpert to existing home systems, and excludes any Win9x systems since they lack the facilities for the required authentication.

Because the patches are distributed as a Push, using Windows file sharing, there is no ability to resume an interrupted patch distribution or to throttle the transfer. It would have to start again from scratch and would consume all available bandwidth.

UpdateExpert was designed to managed locally networked systems running NT/2000/XP systems. It is not suitable for patching remote systems due to the authentication and distribution methods used.

The Future

What does the future hold for Patch Management in general, and VPN users in particular? The major players in this market are working hard to provide very robust, feature rich, secure products.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

St.Bernard software is working on a pull-based client for their UpdateExpert package. The addition of a pull based client would greatly increase the functionality of this product. With the current 'leaf agent

PatchLink just released[13] version 5 of their product based on the .NET framework. Updated features include support for Server 2003, role-based management, customizable graphical reporting.

Microsoft is planning to revamp its patch system by reducing the number of installers by the end of 2003[14].

Microsoft also announced plans for SUS 2.0 at the 2003 RAS Conference in San Francisco. Mike Nash announced that SUS 2.0 would "include update functionality for a broader set of Microsoft products" but no further details have been released[15].

Microsoft SMS 2003 is currently in beta. It includes the SUS Feature Pack in it's base install thus simplifying the install process. The new Advanced Agent uses http to transfer files, and uses the Background Intelligent Transfer Service (BITS) to allow for bandwidth throttling and the resumption of interrupted transfers. Support for Windows NT is not included in the Advanced Agent, but it is still available through the SMS 2.0 client.

Corporations that currently use SMS will benefit from SMS 2003, but as with SMS 2.0, Microsoft does not recommend anyone try to install it just to handle patches. It's an extremely complex package that can perform almost any task you ask of it, but you have to know how to ask it, and that takes a lot of time and training.

SUMMARY

There is a wide range of options available in patch distribution systems today. To deploy patches effectively to systems distributed across the Internet, it seems obvious that Internet standard protocols are required.

Any system that attempts to utilize Windows Shares for remote patch distribution is doomed to failure. The patches would only be available while the VPN tunnel was active. Since there is no native ability in Windows to resume a file copy, the transfer fails when it is interrupted.

Windows also lacks a native ability to throttle downloads, so any large patches will interfere with the tasks for which the user originally created the VPN connection for. This would quickly result is dissatisfaction, and attempts by the user to circumvent the system.

.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

SUS provides a good basic patching service with minimal management overhead and should be used to augment systems like UpdateExpert and SMS when patching over the Internet. The reporting capability in SMS or UpdateExpert would provide the ability to audit the patches and give an Administrator a good idea of the current state of the network.

Currently, PatchLink and BigFix are the only systems reviewed here that are capable of effectively controlling the entire home computer patch management process in their native form.

---

[1] Hurley, Edward. "Survey: Remote offices, workers get short end of security stick." TechTarget, 02 May 2003 . URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci897087,00.html (02 July 2003)

[2] Salamone, Salvatore. "A look at VPN usage growth and what's ahead in 2003." TechRepublic, 20 Jan 2003. URL: http://www.techrepublic.com/article.jhtml?id=r00520030120sss01.htm (02 July 2003)

[3] Markus, Henry. "Home PC Firewall Guide", 22 June 2003. URL: http://www.firewallguide.com/ (02 July 2003)

[4] Rogers, Larry. "Larry Rogers on Applying Security Patches", 01 April 2001. URL: http://www.cert.org/homeusers/apply_patches.html (02 July 2003)

[5] SANS.ORG. "Virtual Private Network (VPN) Policy." V6.0. URL: http://www.sans.org/resources/policies/Virtual_Private_Network.pdf (02 July 2003)

[6] Microsoft. "Take a closer look". "Microsoft Software Update Services". Microsoft, 2003. URL: http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp#section2 (02 July 2003)

[7] Rolsma, Dan B. "Microsoft Windows Security Patches" "SANS.org Reading Room", 2001 URL: http://www.sans.org/rr/papers/67/273.pdf (02 July 2003)

[8] BigFix Inc. "BigFix Consumer WWW page". 2003 URL: http://www.bigfix.com/website/products/consumer.html (02 July 2003)

[9] BigFix, Inc. "BigFix Patch Manager", BigFix, 2003. URL: http://www.bigfix.com/website/products/patchmanager.html (02 July 2003)

[10] PatchLink Corp. PatchLink WWW site. PatchLink, 2003. URL: http://www.patchlink.com/ (02 July 2003)

[11] Microsoft. SUS Feature Pack and Patch Management. 18 February 2003. URL: http://www.microsoft.com/technet/itcommunity/chats/trans/SMS/sms0218.asp (02 July 2003)

[12] St.Bernard. "UpdateEXPERT". 2003. URL: http://www.stbernard.com/products/updateexpert/products_updateexpert.asp (02 July 2003)

[13] PatchLink. "Press Release for PatchLink Update 5.0". 02 June 2003. URL: http://www.patchlink.com/media_room/pRelease_6_3_03.html (02 July 2003)

[14] Microsoft PressPass, "Microsoft outlines plans to Simplify Secure Computing", 14 April 2003. URL: http://www.microsoft.com/presspass/press/2003/Apr03/04-14RSA2003KeynotePR.asp (02 July 2003)

[15] Keizer, Gregg. "Microsoft Touts Year's Plans For Simpler Security, Patch Management", 15 April 2003. URL: http://www.techweb.com/wire/story/TWB20030415S0005 (02 July 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced