The State of Patching Windows

Rafael Cappas

The State of Patching Windows

GIAC Security Essentials Certification (GSEC)
Practical Assignment

Version 1.4b
Option 1

Rafael Cappas III

May 18, 2004

Abstract

Patching is something that everyone tells you to do but find people really don't understand it. There was a time, not long ago, when security vulnerabilities became known and finding patches for them were difficult. One had to scour Usenet looking for further information and dig through FTP servers for fixes. It was pretty much up to the systems administrator to read through the readme files and figure out what it was they had to do to secure their systems. Times have changed, and now the process has been improved but not perfected.

We will look at why we need to patch our systems to make them more secure. I will also cover the types of patches available, and how to find and apply them today. In addition, tools, methods and recommendations will be discussed. The main focus is Microsoft Windows XP and Server 2003, although some portions are applicable to many operating systems.

Patch We Must

Unfortunately every modern operating system had some kind of security patch issued, whether it was for a local or remote vulnerability. Many debate on the cause of so many vulnerabilities and Microsoft tends to be the canned response. Here are some of the more typical answers that may apply to every OS and software – bad programming practices, code reuse, excessive integration, insufficient code review, lack of thorough testing, and rushing to market. All developers should accept responsibility for producing insecure code and need to correct their flaws. A much better approach would be to prevent bad code from appearing in their products in the first place before governments get involved in the process.[1]

Another factor behind the quantity of security flaws discovered is due to the vast use of computers by people today. Many of these systems are running an outdated OS and software, misconfigured, have default or full installations with unneeded services running, never been maintained or were updated at one time, and probably have weak or no passwords. Adding insult to injury, the owners probably do not have any other protective measures (antivirus, firewall, IDS) in place to mitigate the dangers of having these haphazard installations connected to the Internet.[2] What we have here is a vast playground for people to test their wares, no matter what operating system.

Microsoft operating systems have a dominant presence on the Internet and their sheer numbers make them a prime target.[3] Now if you were someone with malicious

[1] Fisher, Dennis. "Clarke: Hold Developers Accountable for Software Insecurity." 14 May 2004.
URL: http://www.eweek.com/article2/0,1759,1592964,00.asp (18 May 2004).
[2] Leyden, John. "US.biz practicing Homeland inSecurity." 11 May 2004.
URL: http://www.theregister.co.uk/2004/05/11/homeland_insecurity_survey/ (18 May 2004).
[3] "Browser Statistics." URL: http://www.w3schools.com/browsers/browsers_stats.asp (18 May 2004).
"Google Zeitgeist – Search patterns, trends, and surprises according to Google." 14 May 2004.
URL: http://www.google.com/press/zeitgeist.html (18 May 2004).

intentions, would you waste your effort trying to exploit 100 thousand machines when you have 1 million to choose from? Do you have intimate knowledge of the UNIX operating system, networking protocols and know at least a couple programming languages to attack a UNIX, UNIX-like, or niche OS? Or would you rather have easy to use GUI tools and scripts to get the most bang for your hack?

With these questions in mind and for other reasons like the 'ease of use' factor, it's simple to see why Windows is the target of choice. Take Windows out of the picture and you'll soon see the next target of opportunity, perhaps the second largest installed base. The skill level bar will be raised again for attackers as it once was in the old UNIX days. Many will drop from the game because of the greater challenge and their lack of mad skillz, but they'll return once all eyes start focusing on the new target and develop easy to use tools.

In Patch We Trust

There are many types of patches, from application and operating system to updates for hardware firmware and a system's BIOS. Patches can be used to add functionality, features, improve performance, or correct software flaws. Our focus is on patches that enhance or add security to the OS and those that address security issues.

There are different names used to describe "software updates" and I will vary them throughout this document.[4] The type of patch you will most likely see is called the Security Update. You can have a single patch that corrects one issue, but add up when many are released. Hotfixes can also address one issue or several as previous updates have shown. Another type is a Quick Fix Engineering (QFE) patch and usually used to address specific problems that may require further testing. Cumulative updates normally include previous fixes and new fixes within a component or program that routinely need updating. Then you have Rollups and Update Rollups consisting of patches that have been deployed for some time and tweaked during the period. This type of rollup is preferable to the just released (not customer tested) bundle mentioned next.

There have been patches that attempt to fix several flaws in one bundle lately. Although this method is probably designed to keep patch counts low and relieve the burden of managing multiple installations, it is not without its faults.[5] Integration of various patches can lead to problems because of dependencies within the bundle. What happens when you only want to install four of the five patches and find out your server does not boot after a successful installation? After troubleshooting your dead

---

"Microsoft's Windows dominates the OS market on the web according to OneStat.com." 24 Sep. 2003. URL: http://www.onestat.com/html/aboutus_pressbox24.html (18 May 2004).

[4] "Description of the standard terminology that is used to describe Microsoft software updates." V6.0. 5 May 2004. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;824684 (18 May 2004).

[5] Roberts, Paul. "Microsoft SSL patch creating SSLowdowns." 29 Apr. 2004. URL: http://www.infoworld.com/article/04/04/29/HNmsftpatch_1.html (18 May 2004).

machine and searching for a solution, you find out that the culprit was the fifth patch you did not want in the first place. Now you get to enjoy recovering your server by uninstalling the patch or reverting to last night's backup. You do have backups that work, right? The server is back on-line but you remain a target to all the vulnerabilities because of that one hole you did not need to plug. You then implement any workarounds available to help mitigate the risks and patiently wait for an updated fix.

This is but one of many possible problems with integrating several different types of patches into one bundle. There are methods to extracting patch bundles and installing select patches but they may come back to bite you in the future, especially if you use automated processes that rely on bundles being intact. I would rather have one patch that corrects the issue at hand and deal with the volume than be subjected to a one size fits all solution.

And then you have Service Packs. These usually contain most previous security fixes along with other system enhancements and stability patches. Some Service Packs also include new features that may or may not be widely known. Microsoft has shifted their decision about including or not including new features in service packs. This is a mixed bag depending who you talk to. It would be nice if one could choose what newly added features were installed during the SP install routine. A potential problem I see with having an option like this would be version nightmares – SP2.1, SP2.2, SP2.2a etc.

Let's not forget the patch from hell…the one that just breaks stuff. People have wasted time troubleshooting problems to later find out that the patch itself had flaws. So the bad fix had to be uninstalled and customers waited for the patch to the patch. There probably have not been as many of these 'types' of patches as many people wish to believe. A good number were possibly self-inflicted by customers themselves. There are usually workarounds to some patches that can be applied until a stable fix is reintroduced.

I can not stress enough the importance of reading the security bulletins associated with patches and service packs. Important information regarding specific configurations that may or may not apply to every OS, known issues of the product after installation, software dependencies, manual intervention to completely correct the issue and much more are there to save you from patch hell. One of the first things I look for in a bulletin is if the patch replaces a previous patch so I can update my listings and archive the old patch. Issues I do have with the patch replacement information is how the wording has changed (searching for superseded was much easier), the section has been known to move to different locations within the bulletin, and then there are times when there is no mention of replacement even though there are bulletins that have "none" in that section. All is not rosy though, I have seen instances where the SP documentation never (or did) mentioned certain previous fixes and later found that they would be included in a future service pack release. A listing of all issues addressed should be included, but not always as history has shown.

The bulletin format has recently been changed a few times and written for both home users and IT professionals. Microsoft has dramatically improved their documentation, although they tend to be revised frequently at times. Browsing through their Security Bulletin Search listing will not inform you of changes to the bulletin, just when the bulletin was issued. Unfortunately you would have to visit each bulletin link to see if any changes were made to the documentation or the patch itself. I highly recommend you subscribe to the Microsoft Security Notification Service (http://www.microsoft.com/technet/security/bulletin/notify.mspx) to be alerted when new bulletins are issued and when patches are updated. Too bad Microsoft doesn't send notices about updates to the bulletins themselves.

Microsoft used to release security bulletins and patches as fixes became available and based on the probability of the vulnerabilities being exploited.[6] A change was made by the company and now it releases bulletins and fixes on a monthly schedule. Microsoft stated that they would release out of schedule patches if there was a risk to justify it. One such instance was the release the MS04-004 patch. Was this move a way to ease the administrative burden on admins and be able to 'plan' patch days? Or was it a way for them to consolidate patches and keep the total body count low? There is speculation on their decision and that is not my topic of concern.

Several things concern many security shops with their recent decision. Patches should become available as they once were and let their customer's security teams decide what schedule they should follow[7]. The black hats have no schedule to follow; the days between vulnerability disclosure and exploits are narrowing. Another problem I see with scheduled updates is the burden on Microsoft's servers during patch day (second Tuesday of the month, 11 a.m. P.T.)[8]. More people are becoming aware of this schedule and automating their systems to grab patches on this important day. Microsoft's servers saw lots of action on April 13 and couldn't keep up with demand. The problem was eventually fixed during the following day, but that was just the first instance. I monitored the May 11 release day and it was thankfully uneventful. Was it because there was only one bulletin and patch released affecting only XP and 2K3? We'll have to wait and see until the next big wave of patches affecting various products is released to see if their servers can handle the load.

Just because a patch is available for your OS does not mean you should install every patch. Blind patching is a major cause of system instability and something that should be taken into careful consideration. Apply updates based on the severity of the problem and if it will have an effect on your situation; you may have processes already in place that can mitigate the risk. Look at the total cost of implementing the solution. Are you a home user and have one box to fix? Does your business have the staff to continually

---

[6] Johansson, Jesper M. "Security Management – April 2004, Oh Patch How I Hate Thee; Let Me Count the Ways." 15 Apr. 2004. URL: http://www.microsoft.com/technet/community/columns/secmgmt/sm0404.mspx (18 May 2004).

[7] Hassell, Jonathan. "Automating Windows Patch Management: Part III." 18 May 2004. URL: http://www.securityfocus.com/infocus/1778 (18 May 2004).

[8] Foley, Mary Jo. "Microsoft Patches: Too Much of a Good Thing?." 14 Apr. 2004. URL: http://www.microsoft-watch.com/article2/0,1995,1567918,00.asp (18 May 2004).

mange less serious risks? How about any changes new updates may have that could decrease the usability of your computers? Do you really need HTML mail? Can your environment tolerate downtime because of a change made with a patch?

Decisions have to be made based on threats, risk, cost and usability.[9] You should have mechanisms in place to be able to decide on actions to take in a reasonable amount of time. Once determined, you can apply patches to test systems, if available, and perform in-house evaluations to see if any negative impacts are present in your environment before rolling into production. Not all situations will apply to every system you have but may affect only some of your configurations. This is the reason why you need to know how every system is configured in your home or business.

A Clean Start

Decide what your requirements (and policies for businesses) are for the system and install the least amount of applications and services from the CD when building a new system. Unfortunately the new operating systems do not allow you to easily customize installations due to the demand from customers wanting everything to work out of the box. OEM systems often ship with restore CDs that have a preconfigured OS and so much other software that prohibit custom reinstallations. You can still remove some components and services after loading.

I would not advise connecting a computer to any network until the latest stable hardware drivers and patches are installed, is hardened and configured with a current anti-virus program and personal firewall/HIDS. Running vulnerability scans and audits would be the next step along with correcting any discrepancies found, and documenting all your hard work. The final step would be imaging or backing up the new build (did you remember to defrag?), and then putting it to work. Your procedures will vary whether you are building for a corporate environment, home or test network. I'll cover how to apply updates if you're not connected to a network later.

Methods to This Madness

We will now take a look at several techniques to patching Windows. The first is doing it the old fashion way, manually locating, downloading and installing each patch. This is tedious, time consuming, subject to error and becomes a nightmare after a couple of machines. The modern approach is built into the OS and called Automatic Updates (AU). AU can be scheduled to automatically check for updates, download, and install them without user intervention, except for the reboot of course. This is the way to go for those who have no desire to get involved with updating their PCs.

[9] Johansson, Jesper M. "Security Management, The Fundamental Tradeoffs." 5 Jan. 2004.
URL: http://www.microsoft.com/technet/community/columns/secmgmt/sm0104.mspx (18 May 2004).

The next process is Windows Update (WU), and is recommended for home users and some small businesses without an IT staff. It's as simple as visiting Windows Update and clicking on Scan Computer. A listing of critical, recommended and other updates will be available after you system has been scanned. Updates considered to be significant by Microsoft will be marked for download and installation. You then can review all the applicable updates and decide which to apply before completing the process of downloading and installing automatically. WU did not always offer you every security patch available in the past and in certain circumstances the same is true today; you may still find yourself manually patching at times.

A more suitable approach for businesses is to install and configure Microsoft Software Update Services (SUS) on a server and manage patches for other servers and clients. This free software is recommended for small to medium sized businesses with IT staff and scales to about 500 clients. Microsoft Systems Management Server (SMS) 2003 and other third-party packages have additional costs and cater to large Enterprises. These two products will not be discussed in detail. The Microsoft Baseline Security Analyzer (MBSA), although a tool designed for businesses will be covered.

Manual Patching: Understanding the Painful Process

Our subject is a default installation from a Windows XP Professional Service Pack 1a CD on an NTFS drive. I chose the default because we are focusing on patching and not hardening a system, and want to demonstrate a typical load. First, you have to know what is installed before you patch.

Windows XP offers much more than a basic operating system. Many programs, components and capabilities are packaged into a complex OS that allow you to do a multitude of tasks. Although many components make up the installation, I will sometimes separate them into different products because they are by their own right another program.

Below is a sample of such products affected by previous security issues:

DirectX
HyperTerminal
Internet Explorer
Media player (three versions included – mplay32, mplayer2, wmplayer)
Microsoft Data Access Components (MDAC)
Microsoft Java Virtual Machine (MSJVM was not included in XP Gold, support was added to SP1 and removed in SP1a)
Microsoft Jet
MSXML
Net Meeting
Outlook Express
Windows Messenger

Windows Script (VBScript, Jscript, Script Components, Script Host, Script Runtime)
.Net Framework

Now that we know some of the things that make up XP, we'll visit the Microsoft Security Bulletin Search web site (http://www.microsoft.com/technet/security/current.aspx). I made some changes to the search criteria to show you how you can filter out the number of bulletins found. The following options were used to obtain the results:

Product/Technology: Windows XP Professional
Service Pack: Windows XP Gold
Update Severity Rating: Critical, Important, Moderate, Low
Bulletin release date: All
Bulletins found: 74

Service Pack: Windows XP Service Pack 1 (changed to)
Bulletins found: 57

Show only bulletins that contain updates that have not been replaced by a more recent update. (box checked)
Bulletins found: 35

Selecting other Product/Technology installed and conducting searches may be needed to get all applicable bulletins. We would then need to cross reference the OS and components and eliminate some bulletins that could be included under the OS category. The count would change once again. Please note that there have been instances where separate updates were issued that needed to be applied from both categories. Direct links to some updates may not be available through bulletins (some links will annoyingly direct you to Windows Update) and you will need to visit the Windows Update Catalog (http://v4.windowsupdate.microsoft.com/catalog/en/default.asp) or Microsoft Download Center (http://www.microsoft.com/downloads) to find them. We will compare the XP and 2003 results with those from automated tools later.

Next is a default installation from a Windows Server 2003 Enterprise Edition CD on an NTFS drive. The server is not configured for any specific role and is standalone. Keep in mind that installed services play a big part in what updates are required and too many variables exist to cover all possible scenarios.

We make another visit to the Security Bulletin Search website for 2003. The following options were used to obtain the results:

Product/Technology: Windows Server 2003, Enterprise Edition
Service Pack: Windows Server 2003 Gold
Update Severity Rating: Critical, Important, Moderate, Low
Bulletin release date: All
Bulletins found: 23

Show only bulletins that contain updates that have not been replaced by a more recent update. (box checked)
Bulletins found: 16

A quick glance at this lengthy process will discourage many people from even considering these procedures. This portion is meant to demonstrate how difficult patching continues to be and a good starting point for those without a process in place. You can begin with manually downloading all the updates and sorting them by whatever criteria you choose, documenting your findings, and maintaining a listing or database of what your clean installation requires. You then construct a system baseline, test, create an image and deploy a consistent load. Now you would only need to maintain future patches and update the baseline as required. Slipstreaming updates and using a RIS server to deploy loads is another method to use in an enterprise. The home or small business user can burn a CD with all this data and build systems without having to connect to the Internet. Users who often build/rebuild their systems and have slow Internet connections can really benefit from having such a CD.

Automatic Updates: Painless Patching

There isn't much to do here…access and configure AU by:

Right clicking My Computer and choosing Properties
Selecting Automatic Updates tab in System Properties window
Checking Keep my computer up to date box
Choosing one of the Settings
Clicking OK

You will need to select your option based on some of the following:

Connection speed
Whether updating will interfere with any tasks being performed at the time
Would rather have the updates done while not using the computer

Now that was easy! This option can satisfy your needs if you are content with everything the server offers you. While AU won't give you all the updates available, it is better than not patching at all.

Windows Update: The Choice is Yours

Launch Internet Explorer and visit http://v4.windowsupdate.microsoft.com/en/default.asp (can also be accessed through the Tools menu). Click on Scan for updates and your computer will be scanned for missing updates. You will see a listing of updates to install for your system on the left and can select which to apply. Most of the critical updates

are security related and selected by default, while the OS section offers recommended and other product updates.

The following results were obtained from a single visit to Windows Update:

	WINDOWS XP	WINDOWS SERVER 2003
Critical Updates and Service Packs	17	15
Windows XP	19	
Windows Server 2003 family		2

Click on Review and install updates once you are finished making your selections and then click on Install Now. A window pops up showing you the download progress and then the install process. The final step for the first visit will be a reboot. You will need to visit WU again after the computer has rebooted to install any additional updates or components that have to be installed separately. Keep revisiting until no further updates are required.

Microsoft Baseline Security Analyzer (MBSA)

MBSA v1.2 is a free tool that can be used to scan local or remote systems for missing security updates and certain types of misconfigurations. MBSA is also used by SUS to scan systems. It is available from Microsoft and can be downloaded at http://www.microsoft.com/technet/security/tools/mbsahome.mspx. The tool uses a signed CAB file that it automatically tries to download when you run a scan. You can manually download the frequently updated CAB file at http://go.microsoft.com/fwlink/?LinkId=18922. MBSA began as a command line utility called HFNetchk and evolved into an easy to use graphical tool. The command line functionally is still present for those wishing to use it with scripts or for other automation tasks. Checks on other software like Microsoft Office, Internet Information Services and SQL Server can also be performed with this tool. Some of the other checks made by MBSA are: passwords, shares, auditing, Internet Explorer zones and potentially unnecessary services installed.

Launch MBSA, click on Scan a computer and then Start Scan. The process will begin by downloading the CAB mentioned above, if you do not have the current version, and then your system will be scanned. Moments later you will be presented with the View security report screen. You'll be able to view the results in the standard brief format or view details within different sections. We will review the Security Update Scan Results.

These following results were obtained with MBSA:

	WINDOWS XP	WINDOWS SERVER 2003
Windows Security Updates	27	12
Windows Media Player Security Updates	1	1
MDAC Security Updates	1	1
MSXML Security Updates	1 (out-of-date)	

Looking at the results between the Security Bulletin Search, Windows Update and the Baseline Security Analyzer, we see slight differences in the number of patches needed to update our systems. The reason for this is the different methods used by the products to analyze their data. Microsoft appears to be consolidating their resources to provide consistent results. I have seen a big improvement in their efforts over the years, especially when the Security Bulletin Search site added the ability to not show superseded bulletins. This option alone saves valuable time by not having to search through all the bulletins to track down which patch is no longer needed. Microsoft still has to refine the automated patch process to make our jobs easier securing our systems.

A Note on User Education

All this work could be wasted if you have users practicing unsafe computing habits. Many jobs today require knowledge of using a computer. As long as the employee knows how to check e-mail, use a couple business applications and can 'surf' the web they are adept. The problem is that all it takes is someone to get an e-mail with a hyperlink and have them click on it. Next thing you know, the person either arrived at a web site running malicious ActiveX, JavaScript etc. code or automatically ran the code within their HTML enabled mail client without them knowing. The user saw nothing happen, deleted the e-mail and life went on for them. How about the telecommuter working from home on the family PC? There's a connection to the corporate office from the same PC little Jimmy uses for his daily dose of peer-to-peer file swapping. Then you have the CFO who's always on the go with her wireless laptop and PDA hoping from one WiFi hotspot to the next. Does she know about WEP or stronger measures that WiFi providers normally don't offer? How about keeping local files encrypted and having strong passwords (or other authentication) on mobile devices (BIOS, disk, login)?

What does this have to do with patching? If you do everything else wrong, patching won't make it right. We need companies to provide some type of indoctrination on the dangers of everyday computing. Most users are probably not going to do it at home. They can start with the basics then have new topics on a monthly basis. Many companies do have security policies in place, but it's just that…a piece of paper someone signs and forgets. Training should be recurring with updated content and performed by the security staff. A trained employee can take that knowledge home and teach little Jimmy a thing or two.

References

[1] Fisher, Dennis. “Clarke: Hold Developers Accountable for Software Insecurity.” 14 May 2004. URL: http://www.eweek.com/article2/0,1759,1592964,00.asp (18 May 2004).

[2] Leyden, John. “US.biz practicing Homeland inSecurity.” 11 May 2004. URL: http://www.theregister.co.uk/2004/05/11/homeland_insecurity_survey/ (18 May 2004).

[3] “Browser Statistics.” URL: http://www.w3schools.com/browsers/browsers_stats.asp (18 May 2004).

“Google Zeitgeist – Search patterns, trends, and surprises according to Google.” 14 May 2004. URL: http://www.google.com/press/zeitgeist.html (18 May 2004).

“Microsoft’s Windows dominates the OS market on the web according to OneStat.com.” 24 Sep. 2003. URL: http://www.onestat.com/html/aboutus_pressbox24.html (18 May 2004).

[4] “Description of the standard terminology that is used to describe Microsoft software updates.” V6.0. 5 May 2004. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;824684 (18 May 2004).

[5] Roberts, Paul. “Microsoft SSL patch creating SSLowdowns.” 29 Apr. 2004. URL: http://www.infoworld.com/article/04/04/29/HNmsftpatch_1.html (18 May 2004).

[6] Johansson, Jesper M. “Security Management – April 2004, Oh Patch How I Hate Thee; Let Me Count the Ways.” 15 Apr. 2004. URL: http://www.microsoft.com/technet/community/columns/secmgmt/sm0404.mspx (18 May 2004).

[7] Hassell, Jonathan. “Automating Windows Patch Management: Part III.” 18 May 2004. URL: http://www.securityfocus.com/infocus/1778 (18 May 2004).

[8] Foley, Mary Jo. “Microsoft Patches: Too Much of a Good Thing?.” 14 Apr. 2004. URL: http://www.microsoft-watch.com/article2/0,1995,1567918,00.asp (18 May 2004).

[9] Johansson, Jesper M. “Security Management, The Fundamental Tradeoffs.” 5 Jan. 2004. URL: http://www.microsoft.com/technet/community/columns/secmgmt/sm0104.mspx (18 May 2004).