

Patch Management: Managing and Maintaining Windows Updates

Sponsored by:



Part 1

Develop a strategy for dealing with security patches

Part 2

Practice effective patch management with Windows Update

Part 3

Stay on top of vital patches with Microsoft's Network Security Hotfix Checker

Part 4

Tips for immediate patch management after a fresh install

Part 5

Keeping software patches up to date with UpdateExpert

Sponsored by:



Develop a strategy for dealing with security patches

As information security awareness has grown over the past few years, the number of patches and updates being released by software vendors has increased considerably. Although this is a positive step in plugging security holes, all of the patches and updates can overwhelm administrators. To help you keep your network up to date, I'm going to outline a simple strategy for managing and deploying these security patches.

Step 1

The first step in managing security patches is to be aware of what issues have been identified and what patches have been released.

Stay updated

The first step in managing security patches is to be aware of what issues have been identified and what patches have been released. The best way to do this is to sign up for Microsoft's [Security Notification Service](#) or to regularly visit the [Windows Update](#) site or the Security section of the [TechNet](#) site. I find the Notification Service the best alternative, since it automatically sends an e-mail when a new bulletin is released. Another advantage of the service is that it covers all Microsoft products, not just the operating systems. The Windows Update service covers only the Windows operating systems.

Let's take a look at a typical security bulletin e-mail ([Figure A](#)) and examine its contents. The first section of the e-mail provides a quick summary of the issue. It identifies the title of the issue, the product affected, the impact, the

Figure A

```
-----
Title:   Flaw in Windows WM_TIMER Message Handling Could Enable
         Privilege Elevation (328310)
Date:    11 December 2002
Software: Microsoft Windows NT 4.0, Windows 2000, and Windows XP
Impact:  Privilege elevation
Max Risk: Important
Bulletin: MS02-071

Microsoft encourages customers to review the Security Bulletins at:
http://www.microsoft.com/technet/security/bulletin/MS02-071.asp
http://www.microsoft.com/security/security\_bulletins/ms02-071.asp
-----

Issue:
=====

Windows messages provide a way for interactive processes to react
to user events (e.g., keystrokes or mouse movements) and communicate
with other interactive processes. One such message, WM_TIMER, is sent
at the expiration of a timer, and can be used to cause a process to
```

A security bulletin e-mail from Microsoft

Sponsored by:



maximum risk, and a bulletin number. Links are provided to the detailed bulletin posted on the Security section of Microsoft's TechNet site. The TechNet page provides a FAQ section and additional details, including a link for downloading the patch.

Evaluate the risk

Read the issue section of the e-mail carefully to find out *exactly* what the issue is and what systems and/or applications are affected. After reading the bulletin, you can evaluate the risk to your organization. The mitigating factors section (**Figure B**) should help with this.

Figure B

```
Mitigating Factors:
=====
- An attacker would need valid logon credentials to exploit the
  vulnerability. It could not be exploited remotely.

- Properly secured servers would be at little risk from this
  vulnerability. Standard best practices recommend only allowing
  trusted administrators to log onto such systems interactively;
  without such privileges, an attacker could not exploit the
  vulnerability.

Risk Rating:
=====
- Important

Patch Availability:
=====
- A patch is available to fix this vulnerability. Please read the
  Security Bulletin at
  http://www.microsoft.com/technet/security/bulletin/ms02-071.asp
  for information on obtaining this patch.
```

Mitigating factors of a security risk

You should answer these questions about the issue:

1. Does it affect software you are using?
2. Do the proper circumstances exist to exploit the vulnerability?
3. If it affects a particular service, can the service be disabled, or can the software be removed without affecting your organization?

After answering these questions, you should be able to decide whether the patch needs to be deployed and to determine the urgency of deployment.

Sponsored by:



Test the patch

Once you have decided that the patch should be deployed, download and test it on a nonproduction machine. Microsoft has a history of releasing patches that end up causing other problems. Of course, a week or so later, a revised edition of the patch is released, but that doesn't help you if the original patch has locked up a critical server.

At the bottom of the bulletin's Web page is a list of revisions to each patch. If the patch will be installed on a critical workstation or server, read the bulletin carefully to ensure that no known hardware incompatibilities exist. Few things can ruin an admin's day like a Blue Screen of Death (BSOD) on a critical server.

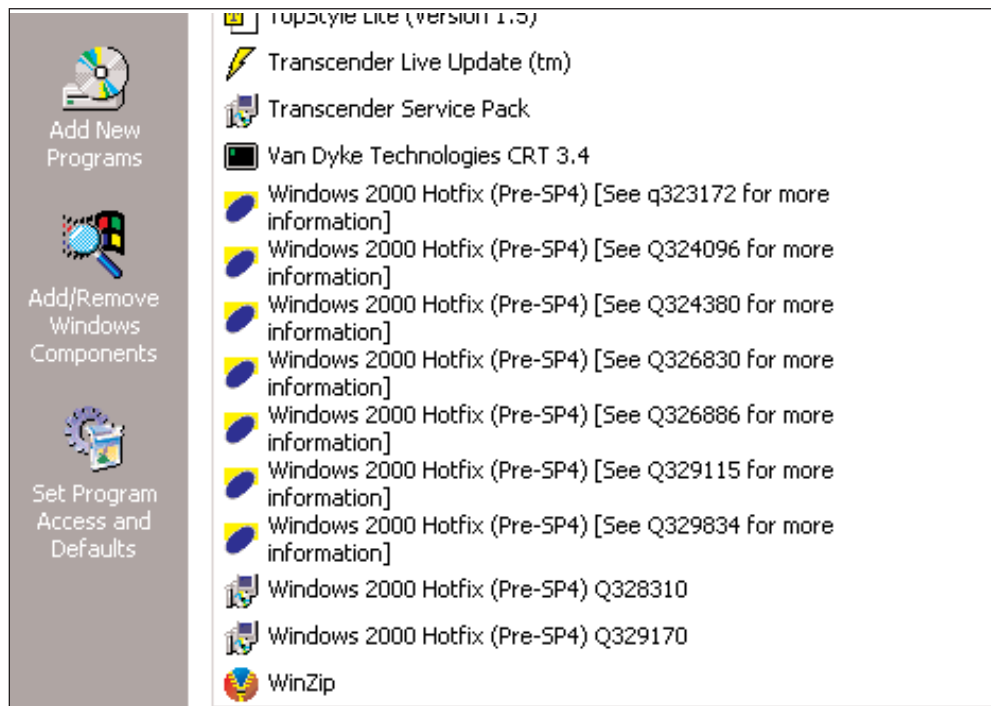
Deploy the patch

By far the most challenging aspect of security patch management is getting the patches installed. In a small organization with a few PCs, manual deployment may be the easiest method of installing patches. For a larger organization, the manual method can be extremely tedious and time consuming. Consider using patch deployment software. This software can remotely scan systems to identify currently installed and missing patches, remotely install patches, and perform reporting and tracking functions. In future articles, I'll cover several patch management software packages.

Author's note

QChain is not needed on post-SP3 Windows 2000 or Windows XP machines, since the hotfix installer on these machines contains functionality to install multiple patches. Most patch deployment software also includes this feature.

Figure C



Deployed patches listed individually in the Add/Remove Programs applet

Sponsored by:



Another headache with manual patch deployment is that a reboot is needed after installation of each patch. Microsoft's [QChain](#) eliminates this problem. QChain is a command-line utility that can link multiple hot fixes together in a single reboot.

Verify installation

After the patch is deployed, you can verify that it's installed correctly by viewing the entry in the Add/Remove Programs applet ([Figure C](#)) or by rescanning the system using patch management software. Each installed patch should contain its own entry, as shown in Figure C.

Summary

The task of managing security patches is not the most glamorous part of IT, but it is an important responsibility that administrators must confront. With a good strategy and the right tools, it can be managed effectively. Next time, we'll look at some of the specific patch management products that can help streamline the deployment process. ♦

Sponsored by:



Practice effective patch management with Windows Update

By Mike Mullins

Patch management is one of the most crucial and intricate parts of Windows security. In the past few years, this issue has mushroomed due to the increased frequency of critical Microsoft patches.

For small business networks, the patch management solution of choice is the Windows Update service. Let's look at how you can manage patches with Windows Update.

Deployment schedule

New patches are available for download on the second Tuesday of each month. The exception is critical releases, which Microsoft publishes as needed. The Windows Update service runs in the security context of the Local System account and starts at the operating system startup (which you can disable). Clients connect automatically to the Windows Update servers and receive a list of missing updates.

Let's look at how you can manage updates via Active Directory and the registry.

Manage updates via Active Directory

With Windows 2000, XP, and Server 2003, you can easily manage Windows Update through group policies. If you don't already have the Wuau.adm template, download it from Microsoft, and save it to the C:\Windows\inf folder on the Active Directory (AD) domain controller.

To load policy settings by using Group Policy in Active Directory, follow these steps:

1. On the AD domain controller, go to Start | Run.
2. Type *dsa.msc* to load the Active Directory Users And Computers snap-in.
3. Right-click the organizational unit or domain in which you want to create the policy, and select Properties.
4. On the Group Policy tab, select New.
5. Enter a name for the policy, and click Edit.
6. Under either Computer Settings or User Settings, right-click Administrative Templates, choose Add/Remove Templates, and select Add.
7. Enter the name of the Automatic Updates .adm file (for example, windows\inf\wuau.adm), and click Open.

"Patch management is one of the most crucial and intricate areas of Windows security."

Sponsored by:



This creates the following entries in the Computer Configuration | Administrative Templates | Windows Components | Windows Update folder:

- **Configure Automatic Updates:** Choose from one of three options: notification for both download and installation, automatic download and notification for installation, or automatic download and scheduled installation. If you select the third option, you can also specify an installation schedule.
- **Specify Intranet Microsoft Update Service Location:** This entry is necessary only if you're running a Software Update Services server.
- **Reschedule Automatic Updates Scheduled Installations:** This determines when the system should reapply scheduled updates that didn't occur according to the schedule.
- **No Auto-restart For Scheduled Automatic Updates Installations:** This blocks automatic startup after installing patches that require a restart to complete.

In addition, the User Configuration | Administrative Templates | Windows Components | Windows Update folder contains a single entry: Remove Access To Use All Windows Update Features. If enabled, this disables user-initiated downloads from the Windows Update Web site.

Manage updates via the registry

On any Windows 2000, XP, or Server 2003 system, go to Start | Run, type *regedit.exe*, and click OK. Navigate to HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU.

Add the following settings. (All value types are Reg_DWORD.)

- NoAutoUpdate
- Value data: 0 or 1
- 0 enables Automatic Updates. (This is the default.)
- 1 disables Automatic Updates.
- AUOptions
- Value data: 2 to 4
- 2 notifies of download and installation.
- 3 automatically downloads and notifies of installation.
- 4 automatically downloads and schedules installation.
- ScheduledInstallDay
- Value data: 0 to 7
- 0 specifies every day.

Sponsored by:



- 1 through 7 designate a specific weekday, where Sunday is 1 and Saturday is 7.
- ScheduledInstallTime
- Value data: n, where n equals the time of day in a 24-hour format (i.e., 0 to 23).
- UseWUserver
- Value data: Setting this value to 1 configures Automatic Updates to use a server that runs Software Update Services instead of Windows Update.
- RescheduleWaitTime
- Value data: m, where m equals the amount of time in minutes (i.e., 1 to 60) to wait before proceeding with a scheduled installation.
- NoAutoRebootWithLoggedOnUsers
- Value data: 0 or 1
- 1 specifies that Automatic Updates doesn't automatically restart a computer while users are logged on.

Note: Editing the registry is risky, so be sure you have a verified backup before making any changes.

Final thoughts

Windows Update depends on the rights of logged-on users. If you decide to use notifications and let users decide which updates to download and install, updates will fail if a user doesn't have local admin privileges.

I recommend always scheduling automatic download and installation. That way, your updates won't depend on logged-on users. ◆

Sponsored by:



Stay on top of vital patches with Microsoft's Network Security Hotfix Checker

As the recent outbreaks of the Code Red and Nimda worms have aptly demonstrated, it is critical for Windows administrators to stay up to date on security patches. To aid in this process, Microsoft has released the Microsoft Network Security Hotfix Checker. This tool allows administrators to scan Windows systems to ensure that all security patches are applied and current.

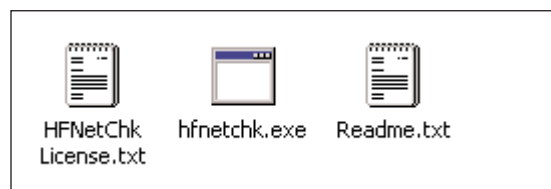
The Hotfix Checker is a command-line tool that looks at the status of all patches installed on your Microsoft servers and tells you whether they're up to date. The tool does this by referring to a public XML database that Microsoft updates periodically. You can use this tool to provide the patch status of the following products:

- Windows 2000
- Windows NT 4.0
- Internet Information Services (IIS) 4.0 and 5.0
- Internet Explorer (IE) 5.01 and higher
- SQL Server 7.0 and SQL Server 2000

Installing and using the tool

When you download the tool, you are prompted for a location to install the executable. Choose the appropriate directory and run the executable. [Figure A](#) shows the files that will be placed in your specified directory.

Figure A



Sponsored by:



To run the Hotfix Checker:

1. Open a command prompt and change to the directory where you installed the Hotfix Checker, as shown in [Figure B](#).
2. Type `hfnetchk`, press [Enter], and you'll see the screen shown in [Figure C](#).
3. For a more detailed explanation, type `hfnetchk -v -z`, as we've done in [Figure D](#).

Figure B

```

C:\WINNT\System32\cmd.exe
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

G:\Documents and Settings\Administrator>cd c:\temp

C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is D0FE-D795

Directory of C:\temp

09/25/2001  12:36p    <DIR>          .
09/25/2001  12:36p    <DIR>          ..
08/14/2001  01:44p                13,346  HFNetchk License.txt
08/16/2001  01:10a                313,712  hfnetchk.exe
08/16/2001  01:45a                 402  Readme.txt
           3 File(s)                327,460 bytes
           2 Dir(s)      5,051,031,552 bytes free

C:\temp>
    
```

Figure C

```

C:\WINNT\System32\cmd.exe
G:\Documents and Settings\Administrator>cd c:\ten
The system cannot find the path specified.

G:\Documents and Settings\Administrator>cd c:\temp

C:\temp>hfnetchk
Microsoft Network Security Hotfix Checker, 3.1
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com <www.shavlik.com>

** Attempting to download the XML from http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab. **

** File was successfully downloaded. **

** Attempting to load C:\temp\mssecure.xml. **

Using XML data version = 1.0.1.145 Last modified on 9/11/2001.
Scanning MYCO
-----
Done scanning MYCO
MYCO
-----

WINDOWS 2000 ADVANCED SERVER SP2

Patch NOT Found MS00-079          Q276471
Patch NOT Found MS01-007          Q285851
Patch NOT Found MS01-013          Q285156
WARNING      MS01-022          Q296441
Patch NOT Found MS01-031          Q299553
Patch NOT Found MS01-036          Q299687
Patch NOT Found MS01-037          Q302755
Patch NOT Found MS01-040          Q292435
Patch NOT Found MS01-041          Q298012
Patch NOT Found MS01-046          Q252795

C:\temp>
    
```

Figure D

```

C:\WINNT\System32\cmd.exe
Using XML data version = 1.0.1.145 Last modified on 9/11/2001.
Scanning MYCO
-----
Done scanning MYCO
MYCO
-----

WINDOWS 2000 ADVANCED SERVER SP2

Patch NOT Found MS00-079          Q276471
File C:\MINNT\system32\hticons.dll has an invalid checksum and
its file version is equal to or less than what is expected.

Patch NOT Found MS01-007          Q285851
File C:\MINNT\system32\winlogon.exe has an invalid checksum an
d its file version is equal to or less than what is expected.

Patch NOT Found MS01-013          Q285156
File C:\MINNT\system32\els.dll has an invalid checksum and its
file version is equal to or less than what is expected.

WARNING      MS01-022          Q296441
The XML file does not contain any file or registry details for
this patch. As a result, this tool is unable to confirm tha
t this patch has been applied. Please verify patch installati
on or refer to Q303215 for more information.

Patch NOT Found MS01-031          Q299553
File C:\MINNT\system32\tlntsvr.exe has an invalid checksum and
its file version is equal to or less than what is expected.

Patch NOT Found MS01-036          Q299687
File C:\MINNT\system32\advapi32.dll has an invalid checksum an
d its file version is equal to or less than what is expected.

Patch NOT Found MS01-040          Q292435
File C:\MINNT\system32\drivers\tdipx.sys has an invalid checksu
m and its file version is equal to or less than what is expecte
d.

Patch NOT Found MS01-041          Q298012
File C:\MINNT\system32\caterp.dll has an invalid checksum and
its file version is equal to or less than what is expected.
    
```



Now that you have a detailed report on your system, you can begin to download and apply the appropriate patches. I recommend that you go to [Microsoft's Knowledge Base Search](#) and enter the appropriate article numbers to find the patches that the Hotfix Checker indicated that you need. After finding a patch, download and install it. I'll walk you through an example to show you what I'm talking about.

To obtain and install patches:

1. As you saw in Figure D, our sample report details many security holes. We'll highlight an article number ([Figure E](#)) and copy it.

Figure E

```
WINDOWS 2000 ADVANCED SERVER SP2
Patch NOT Found MS00-079      Q276471
File C:\WINNT\system32\hticons.dll has an invalid checksum and
its file version is equal to or less than what is expected.
```

2. Next, we'll go to Microsoft's Knowledge Base Search, select Specific Article ID Number, paste the article number in the My Question Is text box, as shown in [Figure F](#), and click Go.

Figure F

Knowledge Base Search
Search the Microsoft Knowledge Base of technical support information and self-help tools for Microsoft products.

1 **My search is about:**
Select a Microsoft product

2 **I want to search by:**
 Keyword Search using All Words
 Specific article ID number
 Specific driver or downloadable file
 Specific troubleshooting tool
 Asking a question using a free-text query
 What's new within the last 7 day(s)

3 **My question is:**
Q276471 go
My last 10 searches

3. At this point, we just downloaded and installed the patch. When we ran the Hotfix Checker again, the installed patch no longer appeared in the report, as shown in [Figure G](#).
4. You can also view the XML file by browsing to where you installed the tool. As you can see in [Figure H](#), there is now another file called mssecure.xml, which you can open and examine.

HotFix Checker syntax

So far, we've covered just the default configuration of this tool. To take a further look at the syntax of the command and its options, type `hfnetchk /?` from the command prompt, as shown in [Figure I](#).

Sponsored by:



Figure G

```

WINDOWS 2000 ADVANCED SERVER SP2
Patch NOT Found MS01-007          Q285851
File C:\WINNT\system32\winlogon.exe has an invalid checksum and
its file version is equal to or less than what is expected.

Patch NOT Found MS01-013          Q285156
File C:\WINNT\system32\els.dll has an invalid checksum and its
file version is equal to or less than what is expected.

WARNING      MS01-022          Q296441
The XML file does not contain any file or registry details for
this patch. As a result, this tool is unable to confirm that
this patch has been applied. Please verify patch installation
or refer to Q303215 for more information.

Patch NOT Found MS01-031          Q299553
File C:\WINNT\system32\lntsvr.exe has an invalid checksum and
its file version is equal to or less than what is expected.

Patch NOT Found MS01-036          Q299687
File C:\WINNT\system32\advapi32.dll has an invalid checksum and
its file version is equal to or less than what is expected.

Patch NOT Found MS01-040          Q292435
File C:\WINNT\system32\drivers\tdipx.sys has an invalid checksum
and its file version is equal to or less than what is expected.

Patch NOT Found MS01-041          Q298012
File C:\WINNT\system32\catsrv.dll has an invalid checksum and
its file version is equal to or less than what is expected.

Patch NOT Found MS01-046          Q252795
File C:\WINNT\system32\drivers\irda.sys has an invalid checksum
and its file version is equal to or less than what is expected.
    
```

Figure H

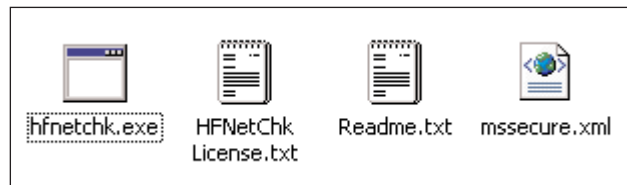


Figure I

```

C:\WINNT\System32\cmd.exe
C:\temp>hfnetchk /?
Microsoft Network Security Hotfix Checker, 3.1
Developed for Microsoft by Shavlik Technologies, LLC
Info@shavlik.com <www.shavlik.com>

hfnetchk.exe [-h hostname] [-i ipaddress] [-d domainname] [-n] [-r range]
              [-a action] [-t threads] [-o output] [-x datasource] [-z] [-v]

Description:
The HFNETCHK tool assesses a machine or group of machines for security
hotfixes that have either been installed and/or need to be installed.
For more information on this tool, please refer to Microsoft Knowledge
Base Article Q303215.

Parameter List:
-h hostname    Specifies the NetBIOS machine name to scan.
               Default is the localhost.
-i ipaddress   Specifies the IP address of the machine to scan.
-r range       Specifies the IP address range to be scanned,
               starting with ipaddress1 and ending with
               ipaddress2 inclusive. <ipaddress1-ipaddress2>
-d domain_name Specifies the domain name to scan. All
               machines in the domain will be scanned.
-n network     All systems on the local network will be
               scanned. (i.e., all hosts in Network
               Neighborhood)
-a action      Displays (i)nstalled hotfixes,
               (m)issing hotfixes, (n)ecessary hotfixes or
               (b)oth installed and missing. Default will
               display necessary hotfixes.
-t threads     Number of threads used for executing scan.
               Possible values are from 1 to 128. Default is 64
-o output      Specifies the desired output format.
               (tab) outputs in tab delimited format.
               (wrap) outputs in a word wrapped format.
               Default is wrap.
    
```

Sponsored by:



Final word

For Windows administrators, this is a powerful tool that enables you to take control of all your Microsoft server vulnerabilities. You can find out more about the Hotfix Checker by reading “Frequently Asked Questions about the Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool.” For an advanced GUI version of the Hotfix program, check out Shavlik Technologies, the company that created the program for Microsoft. ♦

Tips for immediate patch management after a fresh install

By Brien M. Posey, MCSE

Over the last several years, patch management has become a huge issue for Windows machines. Microsoft constantly releases patches not only for the operating system, but also for server applications such as Exchange Server and SQL Server. Keeping up with patches is one thing, but you also need to consider patch management any time that you deploy a new server. Remember: In a way, a server is most vulnerable immediately after it is brought online. This is because no patches have been installed to counteract known security or stability issues. Here's everything that you need to know about installing patches on new servers.

Patches vs. service packs

Before I get started, I want to take a moment and discuss the differences between patches and service packs. During the years that I have been involved in IT, I have noticed a strange phenomenon regarding patches and service packs. It seems that often administrators are extremely anxious to apply patches the instant they come out. On the other hand, when a new service pack is released, those same administrators will often wait weeks, if not months, to apply it.

In a way, I can understand the rationale behind this. A patch is a small fix that's usually designed to fix some critical security hole or system stability issue. A service pack, on the other hand, tends to replace the majority of the operating system's files. It's only natural to be distrustful of a service pack that is going to overwrite the majority of the system files that your operating system uses. People usually want to wait a little while and see if anyone else has problems with the service pack prior to applying the fix themselves.

The ironic part is that this approach is exactly opposite of what Microsoft recommends. According to a [Microsoft TechNet article](#), the biggest difference between patches and service packs is that service packs are planned and patches are not. According to the article, before Microsoft ever releases a new service pack, they test it for weeks against hundreds, if not thousands of third party applications. The article states that Microsoft service packs meet the same quality standards as the operating system itself (okay, stop laughing).

On the other hand, patches are released on an as-needed basis. For example, if some big security hole were discovered tomorrow, Microsoft would very quickly produce and release a patch for the problem. The patch would

Sponsored by:



have undergone a minimal amount of testing, but remember that Microsoft's goal is to make the patch available quickly, not to test the patch for every possible situation. Therefore, there have been a lot of cases where patches have been unstable.

When a service pack is released, all of the bugs and security problems that have been discovered and patched since the last service pack are included in the new service pack. The difference is that the service packs are thoroughly tested. Therefore, although a new service pack might fix the same bug as a previously released patch, the service pack might use very different code to fix that bug from what was originally released in the patch.

Patching a new server

As I explained earlier, when a new server is initially brought online, it is at its most vulnerable because it contains no patches. Therefore, I recommend installing the most recent service pack immediately after installing the operating system onto the new server.

Once the service pack is installed, I recommend installing your antivirus software next. The third step that I recommend taking is to update your virus definitions. Next, install any server-level applications such as Microsoft Exchange or SQL Server. Finally, install the latest service packs that exist for your server applications.

Following those steps should make the server relatively secure. Keep in mind, though, that Microsoft releases patches for operating systems and for applications on a regular basis. Therefore, you will want to apply the patches that have been released since the most recent service pack. Because patches receive minimal testing, you will have to make a judgment call; you can either install every available patch or you can install only those patches that fix severe security vulnerabilities or that address issues that directly affect you.

There are good arguments for both sides of this issue. Some people believe that if a vulnerability exists then it should be patched. Period. On the other hand, other people believe that since patches are created on the fly and are largely untested, it's better to preserve system stability by applying only the patches that you really need. In my opinion, the correct approach depends on your organization. Anyone in a high-security environment, such as the military or a financial institution, probably wants to apply every patch the instant that it becomes available. The rest of us are probably OK picking and choosing though.

What patches do I need?

One question that I tend to get asked a lot is that if Microsoft is constantly releasing all of these patches, how can you figure out which patches you really need. More importantly, where do you get these patches. About a year or

Sponsored by:



two ago, Microsoft released a tool to make patch management much easier. The tool is called the Microsoft Baseline Security Analyzer (MBSA).

The Microsoft Baseline Security Analyzer

The MBSA is a utility that analyzes your server to see which security patches have been applied. It then compares the list of detected patches against a list of available patches that's contained in an online database. Because the database exists on the Internet, Microsoft can keep it up-to-date. Therefore, you can periodically run the MBSA and see if there are any critical updates that you might be missing.

The MBSA doesn't come with Windows, but you can get it by downloading it from [Microsoft's Web site](#). The download consists of a 3774 KB MSI file. This means that you can install the utility on Windows 2000, Windows XP, or Windows Server 2003. The installation procedure consists of running a very simple wizard. You can install the utility onto any Windows system, as long as that system has a network link to the computers that you want to test the security for. The utility requires about 3 MB of disk space.

When the installation completes, you will see the main MBSA screen, shown in [Figure A](#). As you can see, the MBSA's user interface allows you to scan a single computer, multiple computers, or to view reports created during previous scans.

Figure A



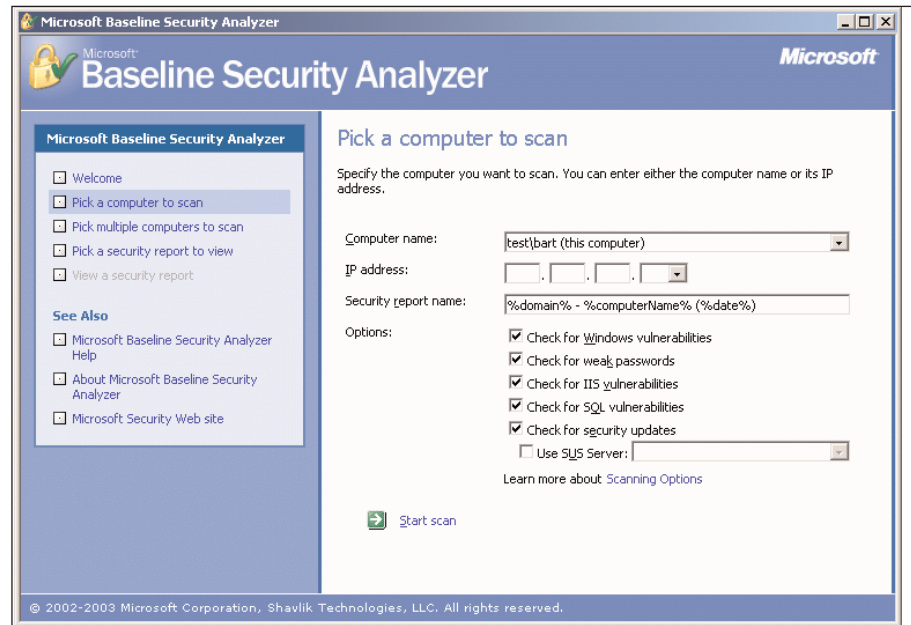
This is the MBSA user interface

At this point, you'll see the screen that's shown in [Figure B](#). This screen allows you to set the various scanning options. First, you must select which computers that you want to scan. You may either enter the name of the

Sponsored by:



Figure B



You can scan multiple computers based on domain name or on IP address.

domain that you want to scan, or you can enter a range of IP addresses. Using an IP address range tends to be more effective if you have multiple domains that you want to scan. Just keep in mind that the account that you're logged in with must have administrative privileges on the machine that you're scanning. Therefore, simultaneous scans of multiple domains will fail unless the account that you're using has administrative privileges in all domains.

Regardless of which method you use, you need to know that the utility won't scan all of the computers within the domain or IP address range. The utility will scan only machines that are running Windows NT, Windows 2000 (Professional, Server, and Advanced Server), Windows XP (Professional and Home Edition) and Windows Server 2003.

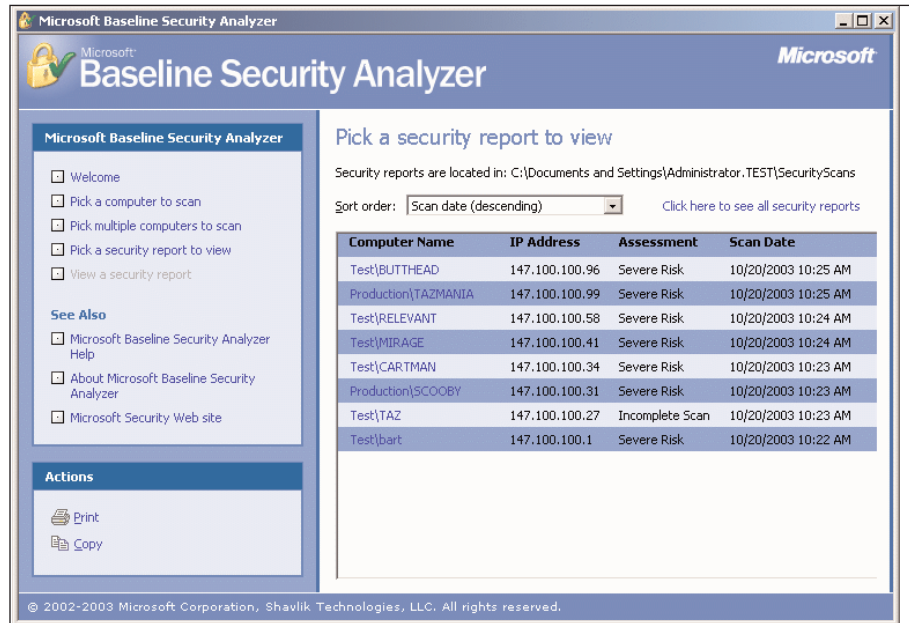
Beneath the IP address range field is the Security Report Name field. By default, the security report name is set to %domain%- %computername% (%date%). In this report name, the %domain%, %computername%, and %date% variables would be replaced by the actual domain and computer name and the date. Even if you're testing by IP address, the report name format is OK to use, because rather than generating one large report, the utility generates a separate report for each computer that it analyses.

At the bottom of the window are the various scanning options. As you can see in the figure, several check boxes allow you to control whether or not things like Windows vulnerabilities and weak passwords are tested. Select the desired scanning options and click the Start Scan button

Sponsored by:

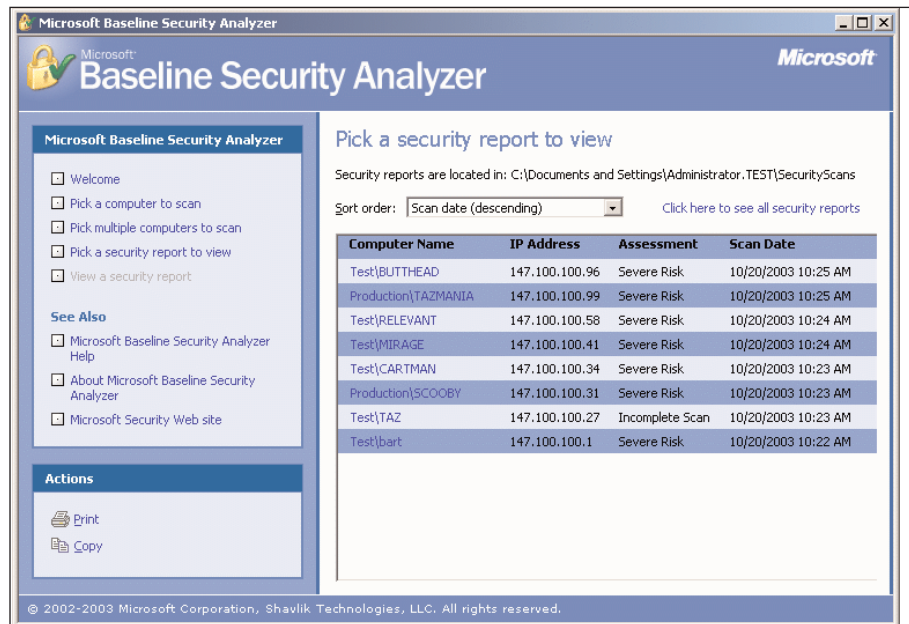


Figure C



You can tell at a glance which machines have problems.

Figure D



Twenty-nine Windows security updates are missing from my test machine.

When the scanning completes, you'll see a list of the systems that were either completely or partially scanned. As you can see in the Assessment column in **Figure C**, the utility tells you instantly what machines need the most attention. In this particular case, the machine Bart, which was diagnosed as a severe risk, is a Windows 2000 Server running Service Pack 3 but no other patches.

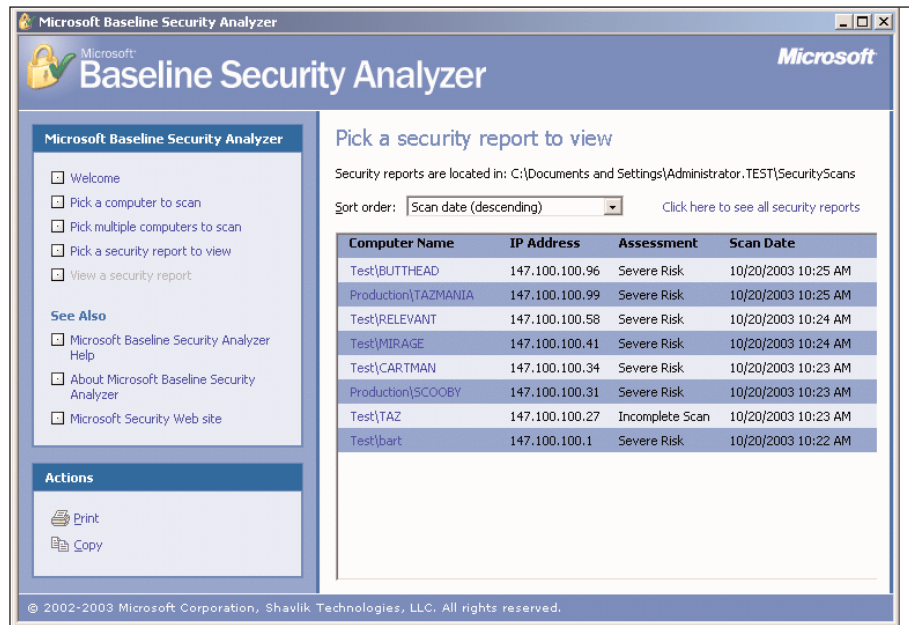
Sponsored by:



Now, let's look at an actual report of the machine that was determined to be a high risk. You can do so by simply clicking on the computer name. The report is much too long to fit onto a single screen. However, in **Figure D** you can see the top portion of the report. Notice that each issue is scored with a red X (danger), a yellow X (caution), or a green check mark (good). Beneath each issue are links for what was scanned in the particular test, the result details, and how to correct the issue. For example, in Figure D you can see that the report indicates that 29 Windows security updates are missing from my test machine.

Of course, just knowing that there are 29 updates missing isn't enough; you need to know which updates so you can do something about it. If you click on the Result Details link, you will see a screen similar to the one in **Figure E**. This screen contains a description of the problem and the reason why it was detected (it's usually a matter of the existing file version vs. the correct file version of an operating system file). There is also a link to the Microsoft Knowledgebase article that describes the problem in more detail. Most of the time these Knowledge Base articles also have links for downloading the missing security patches.

Figure E



Sponsored by:



You can get a detailed explanation of which patches are missing and how important each patch really is.

Hopefully by now you have decided which service packs and patches you want to use and have applied them. By now your antivirus software should also be installed and up-to-date. The next step is to make a backup or a ghosted image of the server.

Ghosting

No one plans on reformatting a server after a fresh install, but it does happen. Over the years, I have seen a number of situations in which shortly after a server was brought online it had to be taken right back offline because of some critical flaw. In some of these cases a hardware failure was to blame. Perhaps the hard disk failed or bad memory was causing corrupt data to be written to the hard disk. In other cases I have seen people have to reformat a server after a severe virus infection or after a security breach has occurred. My point is that, although you never plan on reformatting a brand new server and starting from scratch, there are situations where it might be necessary.

Because of this, I recommend creating a ghosted image of the server's partitions once all of the patches and server applications are in place. There are two main reasons for doing this. The first reason is that it is a time-saver. Suppose for a moment that your new server had a critical failure tomorrow. It would be much faster to restore a couple of partitions from ghosted images than to reinstall the operating system, patches, and applications completely from scratch.

The other reason for creating a ghosted image is a little more important than just saving time. Remember, between the time that you bring the new server online and the time that you install the various patches, you are vulnerable to whatever security issues those patches might address. It is unlikely that a hacker or a Trojan would compromise your server in this short period of time, but it has been known to happen—especially if you accidentally forget to apply a critical patch.

Ghosting your server guarantees that if you have to restore the image, then the restored image will already contain all of the patches that had been applied up to the time that the ghosted image was created. One might argue that if this image needed to be restored a week after it had been created, then the image would be invalid because several new patches could have come out in the course of that week.

While it is true that more patches could have come out during the time between when you create an image and when you restore the image, I would still recommend using the ghosted image. That's because the ghosted image will already contain a number of security patches. You can simply apply the new ones rather than worry about reapplying all security patches. After all, having some security patches in place is better than having no patches. ♦

Sponsored by:



Keeping software patches up to date with UpdateEXPERT

By Brien M. Posey, MCSE

One of the most frustrating parts of network management is trying to keep up with all of the available patches that should be applied to the various servers and workstations on the network. Patch management can be a huge job. After all, security patches aren't the only types of patches that you need to worry about. It's just as important to apply other types of bug fixes and service packs. Furthermore, there are also patches for applications, not just for operating systems.

To make matters worse, not all patches are reliable. Anybody remember Windows NT Service Pack 6? Microsoft almost immediately replaced it with Service Pack 6A because it caused so many problems. A more recent example is Windows XP Service Pack 2. In certain environments, this service pack triggers incompatibilities and other errors.

To help you with patch management, [St. Bernard Software](#) has released a product called [UpdateEXPERT](#). UpdateEXPERT is a software patch management tool that can automatically apply patches to your workstations and servers. In fact, UpdateEXPERT manages patches for a wide variety of operating systems, applications, and server applications. These include Windows NT 4.0, 2000, XP, Internet Information Server, Terminal Server, Media Player, Windows Media Services, NetMeeting, Microsoft Office, Outlook, and more.

One-stop patch updating

UpdateEXPERT has a unique way of managing patches that seems to get around many common patch management problems. The most obvious problem with traditional patch management is that there are just too many patches to track. Rather than requiring you to visit Web sites for each software package, you can simply check the UpdateEXPERT database for any updates available. The research database is organized into a tree view. This means you can either search for a specific patch in the traditional manner, or you can browse through the tree to see what's available for your specific products.

The best part is that when you're deploying a patch, unstable updates are no longer a factor. St. Bernard Software claims to thoroughly test any available patches for reliability prior to publishing the patch in its database. If you attempt to deploy a patch that UpdateEXPERT considers unsafe, the software will block the installation.

The most obvious problem with traditional patch management is that there are just too many patches to track.

Sponsored by:



Built-in scripts

Another common patch management problem is that in larger organizations, deploying a patch can be time-consuming. Manually deploying a patch to thousands of workstations is simply not an option. In most cases, you can deploy a patch by writing a deployment script. However, it takes time to write and test these scripts—time that your programmers could better spend doing other things. UpdateEXPERT has deployment scripts built in. Each deployment script is written for a specific patch and is tested for reliability. You can use the UpdateEXPERT interface to deploy a patch with just a few mouse clicks.

Profiling patches

Aside from the deployment issues, there are other problems with traditional patch management as well. For example, suppose a new, critical patch became available for Internet Explorer. Obviously, you'd want this patch applied to everyone's computer. How would you know if the patch was actually applied to all those machines? Furthermore, how would you know if someone accidentally removed the patch later on?

UpdateEXPERT solves this problem in a couple of ways. First, it allows you to create a profile of which patches you consider mandatory. You can then query each machine against the applicable profile to see if all of the required patches are installed. Next, you can build a report verifying exactly which patches are on each machine. Of course, you can also have UpdateEXPERT automatically deploy any patches that are missing. Best of all, the tool contains a built-in scheduler. This means you can schedule such operations rather than having to run them manually.

You aren't limited to using a single profile across the entire network. You can create a variety of profiles and assign these profiles to groups of machines. For example, you might create machine groups by operating system, service pack level, or even by a machine's assigned OU within Active Directory.

Accessibility agent

Yet another challenge of traditional patch management is accessibility. For example, suppose you have a Web server that is accessible to the public via the Internet. Since the Internet is such a hostile environment, you've probably taken many steps to make sure the Web server is as secure as possible. The problem is that high security environments usually block any attempts to remotely add any software to the machine.

Normally, when UpdateEXPERT needs to update a machine, it does so with RPC calls. However, in a high security environment or on machines that are tightly locked down, RPC traffic is often blocked. To get around this problem, UpdateEXPERT offers an optional agent component. You can

Sponsored by:



What's new?

One of the software's newest features is that it can be used as a snap-in for HP OpenView. St. Bernard Software is a solution-level member of the [HP OpenView Solution Alliance Program](#). The OpenView plug-in will allow IT managers to effectively inventory, deploy, test, and validate the increasing number of Windows patches.

apply this agent to secure machines, and it will allow the machine to communicate with UpdateEXPERT in spite of other security settings.

In case you're wondering, all components of UpdateEXPERT, especially the agents, are designed to be secure. All UpdateEXPERT transmissions are encrypted and CRC checks are run against patches before the patches are applied. Another nice security feature is that an administrator doesn't have to be logged in with an administrator account in order to apply patches to remote machines. Instead, an administrator can create an account whose sole purpose is patch updates. The administrator can then use UpdateEXPERT to delegate the necessary privileges to that account.

Acquiring UpdateEXPERT

St. Bernard Software has a free trial version of UpdateEXPERT that you can download from http://www.stbernard.com/products/updateexpert/products_updateexpert.asp. This trial software will allow you to test UpdateEXPERT on up to five machines for 15 days. If you decide to purchase the product, you can do so directly from the St. Bernard Software Web site. Pricing is based on a sliding scale determined by the number of licenses and number of years that you subscribe to patch updates.

Sponsored by:



Patch Management: Managing and Maintaining Windows Updates

Sponsored by:



St. Bernard Software

St. Bernard Software Inc. is a global provider of security solutions that protect against data loss, system threats, Internet abuse and unsolicited email. Through its products and services, St. Bernard Software helps companies protect their bottom line by securing networks against major risks before they happen.

One of its premier products is UpdateEXPERT, the patch management solution that automates the time-consuming tasks involved in securely and reliably patching machines on your network.

UpdateEXPERT is not only the easiest-to-use solution, it is also the most cost-effective because there are no dedicated server hardware nor server class machines required and you don't need Internet Information Server to use it. Multiple deployment sites are available at no additional charge.

Here are some of the other outstanding features of UpdateEXPERT:

- **Remotely Manages Any Number of Systems:** With our Optional Client Agent, you can manage your networks in the most effective way possible including machines that are isolated, locked down or unconnected. The Client Agent gives you the flexibility to manage patch deployment, validation and reporting whether you have 4 machines or 4,000.
- **Exclusive Metadatabase:** Users have access to the exclusive metadatabase, which contains the intelligence for how to deploy, validate, install and research thousands of patches. The metadatabase is the result of St. Bernard Software researching and testing all patches to ensure reliable patch management.
- **Knows What You Are Missing And Validates:** UpdateEXPERT includes enhanced patch validation with intelligent version checking functionality that automatically validates files according to checksum, file size and version information. If a new patch overwrites a file from an older patch, UpdateEXPERT knows that the newer file is still valid.
- **Scalable for Small to Large Enterprise Organizations:** UpdateEXPERT is a comprehensive, easy-to-use application that works "off the shelf" for any size organization.
- **Comprehensive Reporting:** The reporting feature lets you share reports among management console users. You can also match your baseline against current inventory and manage by exception.