

Winning the Hotfix Race

Mark Burnett 2000-06-24

Even a Broken Watch is Correct Twice a Day

Any NT or IIS admin is familiar with the process of applying service packs and hotfixes--as well as all the problems associated with it. But the fact is, no software is going to work 100% of the time, especially when you take into consideration the many security concerns of a web server. But Microsoft does not always make it easy on us.

The process of keeping up-to-date can be a time-consuming and often confusing process. First, one must be aware of the issues and the availability of a fix. Then one must determine if the fix should actually be applied to each server. And finally there are the logistical issues of deploying hotfixes to a number of servers. But as long as there is software, there will be hotfixes for that software.

When To Fix

Obviously, a good time to apply service packs and hotfixes is immediately after installing a product on your computer. A fresh install of any OS is considered insecure and is normally full of holes. Windows NT and Windows 2000 are no exception. But applying hotfixes after a fresh install is not going to keep the OS secure. You must keep up with Microsoft Security Advisories in order to stay secure. You must also often reapply service packs and hotfixes when adding or removing certain system components.

But how do you know exactly what needs to be reapplied after which components are added or removed? Keeping track of what changes can be difficult and much of the documentation available can be confusing and sometimes contradictory. Often, many administrators will just reapply all service packs and hotfixes regularly just to be safe. But there are also some third-party tools that may help the process such as SPQuery or Service Pack Manager.

If It Ain't Broke, Don't Fix It

System administrators have many different philosophies when it comes to hotfixes. Some will religiously apply every available fix while others will never touch a system that is already working well. There's a an Italian saying "Una scopa nuova spazza bene" which translates to "A

new broom sweeps well." We all like the new car smell but sometimes new software is not always the best answer. There are systems out there that have 99.9999% uptime but that is only because they are running the same software that was originally installed ten years ago. The proper way to approach the problem is to balance the benefits of a hotfix to the risks of introducing new bugs. I imagine that some hotfixes are nothing more than the software version of duct tape and bailing wire and even Microsoft warns against using all hotfixes unless specifically needed. Most hotfixes have not been fully regression tested so the implications of applying them are for the most part unknown.

So the question is really one of whether you really need the update or not. Often, the security benefits of a hotfix far outweigh the risks of applying the fix. Nonetheless, if the hotfix applies to a service or function that you are not using, you may be better off just not applying it. However, you must keep track of which fixes are applied to a server so that if you ever do use that service or function in the future, you can know to apply the hotfix.

When deciding to apply an advisory it is good practice to review the associated knowledge base article. Every hotfix will be accompanied by a knowledge base article that is often included with the hotfix itself. These articles will usually explain who needs to apply the hotfix and what problems are corrected. Keep in mind, however, that often the article will be vague about the actual exploit, making it difficult to decide if there is another workaround without having to apply the fix. Often, if the bug was discovered by another company and reported to Microsoft, they will have their own advisory that will have much more detail. Check the security mailing lists if necessary to get more information about the hotfix.

Applying the Patch

Once you have determined to install a hotfix, you should download and install it on a test system. Usually this is a non-critical server that has a similar configuration as your main web server. The time spent testing really depends on your resources, time, and risk exposure. Once satisfied with the stability of the patch, you can then plan to put it on your production server. If possible, time the update at a time when your web traffic is low. If you have multiple web servers, only work on one at a time, making sure that one is up and running stable before working on the next.

If you are installing a new server and are applying multiple patches, keep in mind that it is usually important that the fixes be applied in the correct order. Microsoft usually documents

the correct order, but it is not always very clear and can sometimes be difficult to follow. To cope with this, I usually save each hotfix in a directory that includes the Q-number, such as "Q244599 C2-Fix." That way, the hotfixes are for the most part saved in a chronological order and can be reapplied in that same order. It is also important to remember to group them by service packs as well, as the service packs will include most of the previous hotfixes--but not always.

Another good reason for tracking the hotfixes by their Q-number is so that when you are reading the documentation for a service pack, you can easily see which ones are included and which ones are not. Although most hotfixes will be rolled in to the service packs, there are times when a fix may not be best for everyone and so therefore they are not included. You must manually keep track of this and be sure to apply the old hotfixes when necessary.

With the new [Windows Update](#) service, it is quick and easy to keep your system patched. But like the service packs, not all hotfixes are included. The only way to know which ones are included and which ones are not is to use both the Windows Update site as well as the [Security Bulletin](#) site.

Keeping Up With Updates

Keeping up with all the service packs and hotfixes is not as simple as it seems. I have already mentioned Windows Update and the Security Bulletin site, but there are also other places where fixes may be hidden. Here is a list of resources that may be good to check regularly:

Microsoft Sites:

[Windows NT Hotfixes](#) - Hotfixes for Windows NT 4 and 3.51

[Windows NT Service Packs](#) - Service Packs for Windows NT 4 and 3.51

[Windows 2000 Downloads Page](#) - Contains all critical updates, service packs, and other downloads for Windows 2000

[Microsoft's Main Downloads Page](#) - Allows you to search for downloads for any Microsoft product

[Microsoft's FTP Site](#) - FTP access to most product updates, although some are hidden in obscure locations

[Office Update](#) - Downloads and updates for Microsoft Office

[Microsoft's DLL Help Database](#) - Very useful database for tracking down dll versions

Non-Microsoft Sites:

[Paperbits](#) - Excellent update resource for Windows NT as well as third-party drivers

[Versions](#) - Tracks version numbers for a number of software applications

[BugNet](#) - Excellent resource for keeping on top of software bugs

Finally, do not forget [Microsoft's Knowledge Base](#). If you search for the word "Fix:" or "security_patch" and only include articles for the last several days, you can sometimes find fixes that would otherwise sneak by without much notice.

One way to keep on top of all these pages using Internet Explorer is to navigate to the page, then from the favorites menu, select Add to Favorites. Then check the Make available offline button and click on Customize to create a synchronization schedule. I normally set it to synchronize every day. Save the schedule and the bookmark and next time the page changes, a red dot will appear next to the site's icon in the favorite's menu.

Distributing Updates

Keeping on top of updates difficult enough for one or two servers, but if you have to distribute updates to several hundred computers across an enterprise, the task can be quite overwhelming. To do this, I would recommended creating a network share for storing all service packs and hotfixes. To actually distribute them, you may opt to manually apply each one, use a script or batch file, use Microsoft's SMS server, or use some other third-party software. If you have all Windows 2000 systems, you may very well want to consider using ActiveDirectory's publish and assign features to distribute updates. Publish allows you to make updates available for installation and assign will actually force the install on every computer under the control of that policy.

Some day managing service packs and hotfixes will be a thing of the past. But for now you must know about the updates, know that you need to apply them, know where to get them,

reinstall them (and in the right order) after changing your system, and have a good plan for distributing them across your company. Nonetheless, with a good strategy, it can be done and it can be done well.

Relevant Links

[Windows Update](#)

Microsoft

[Microsoft Security Bulletins](#)

Microsoft

[Windows NT Hotfixes](#)

Microsoft

[Windows NT Service Packs](#)

Microsoft

[Windows 2000 Downloads Page](#)

Microsoft

[Microsoft Main Downloads Page](#)

Microsoft

[Microsoft FTP Site](#)

Microsoft

[OfficeUpdate](#)

Microsoft

[DLL Help Database](#)

Microsoft

[Privacy Statement](#)

Copyright 2006, SecurityFocus