Global Information Assurance Certification Paper

Can You Afford Not to Install Windows NT 4.0/Windows 2000 Service Packs and Security Hotfixes
Judy Overhauser-Duett
December 3, 2000

Introduction

Microsoft provides Service packs and hotfixes to update security issues, application hardware/software compatibility issues, setup issues, and operating system reliability [1]. The service packs and hotfixes can be obtained from the Microsoft download site free of charge.

Window 2000 Service Pack 1 (SP1) can be obtained from http://www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp[1] or http://windowsupdate.microsoft.com/ [2]. The service packs can also be ordered from Microsoft for a nominal fee on CD. The CD version includes added customer support diagnostics [1]. I wouldn't recommend downloading unless you have a cable modem or fast link at home. I actually got a cable modem after trying to download a service pack. The download timed out after 14 hours with just five minutes to go. My friend had downloaded the same file in three minutes via cable modem.

The latest Windows NT 4.0 Service Pack (SP6a) can be obtained http://www.microsoft.com/ntserver/support/faqs/sp6faq.asp [3]

The ultimate question is "Can you afford to not install the latest Windows NT or Windows 2000 service pack and or hotfixes?"

Service Packs

Microsoft breaks down service packs into two categories: required (critical) and recommended. Critical updates are those that are critical to the safe/secure operation of Windows NT 4.0/Windows 2000 [2]. Recommended updates are those where Microsoft asks you to review the list of fixes/enhancements to decide whether to apply the service pack. The list of Bugs Fixed in Windows 2000 Service Pack 1 includes all security updates.[5] All updates should be applied and tested on an offline system to ensure they do not break anything. My analysis for determining whether to apply the service pack is to determine how many serious security holes are fixed by the service pack that apply to my systems. If a hole is high risk or the combination of more then one makes my risk unacceptable, I apply the service pack.

Window 2000 SP1 includes the capability to apply the service pack once to a network version of Windows 2000 and then to slipstream this version out to the the whole corporation. All systems are thrn installed with both the base system and SP1 in one installation. SP1 no longer requires reapplying the service pack each time a new device driver is loaded. [1] [6]

Window NT 4.0 SP6a fixed many winsock problems, included all previous security upgrades regression tested, and included the Y2k fix for NT. The Y2K fix was also available separately so the service pack was labeled recommended. The latest NT service pack is available from www.microsoft.com/ntserver.support/faqs/SP6/faqs/sp6fag.asp. [3] In my view if you are running Window NT 4.0 and are connecting to the Internet you should update to Service Pack 6a unless you have a system incompatibility even though it was only stamped a recommended service pack by Microsoft. Be sure and test offline before you put it on a production system.

Hotfixes

Hotfixes are a little different story. Whereas service packs have been regression tested (meaning the application of the service pack had been tested to not break existing code) the hotfix has not. Microsoft warns that you apply hotfixes at your own risk. A few years ago I was supporting Window NT 4.0 at various Department of Defense clients. We went through each of the hotfixes as it was supplied by Microsoft and mandated whether or not it must be applied immediately. Hotfixes for Windows NT 4.0 are a little crazy too. They have to be applied in the specific order they were issued and if you miss one you have to apply it, followed by reapplying those that came after it. The ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt4 gives the post service pack hotfixes [4].

An example of a security update or hotfix that you would have to decide applicability for your company is "account lockout in Windows 2000 bypass"[7]. The particular update fixes the problem where a user with a domain account

can repeatedly fail login and not be locked out. I would not want a domain open to a hacker password attack so I would most likely load this update if successfully tested offline.

Window Update

The http://www.windowsupdate.com site can be used to lessen the pain of determining whether or not there is a critical service pack or hotfix for your home computer or for a small business. The site states its purpose as maintaining "trouble free operation of your computer and to protect your computer from security vulnerabilities" [2]. The site queries your computer to determine what updates have been loaded. It also states that the information is not being sent back to Microsoft. The site could also be used for each computer at a large site but it would not guarantee that all computers were running a standard site installation. I use the site at home. It currently tells me there are three critical security updates for my computer. I just upgraded my operating system to Windows 2000 Professional this weekend but haven't registered yet so it may not be picking up all the correct data from the registry. After I register, I will again check the Windows update site and apply the security updates or hotfixes needed.

The Windows update link also includes a capability to be notified whenever there is a critical update to your system.[2]

Recommendations

Service pack 1 for Windows 2000 is a recommended service pack. Therefore, check the list of updates at the download site. I personally recommend installing all service packs within six months of their issuance if there is no problem found when testing offline.

Without service pack 1, we had an application that would not load on Windows 2000. Once the service pack was loaded, the application loaded flawlessly because of application driver updates added to the service pack. The added features of Windows 2000 SP! for slipstreaming, the fact that you no longer have to reload the SP every time you add a new driver, and the updated application drivers included with the service pack give me enough incentive to load this service pack.

With NT 4.0, I recommend updating to SP6a as stated above under the Service Pack heading even though SP6a is just a recommended service pack.

References

1. Microsoft. URL: http://www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp

2. Microsoft. URL: http://windowsupdate.microsoft.com/.

3. Microsoft. URL: http://www.microsoft.com/ntserver/support/faqs/sp6faq.asp

4. Microsoft. URL: ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt4

5. Microsoft. "Security". List of Bugs Fixed in Windows 2000 Service Pack 1 (3 of 3). URL: http://support.microsoft.com/support/kb/articles/q269/4/28.asp

6. URL: www.windows.2000faq.com/articles/index

7. Manzuik, Steve. "Account Lockout Policy in Windows 2000 Can Be Bypassed". Windows IT Security. 21 Nov 2000. URL: http://www.windows.security.com/Articles/Index.cfm?Article