

Patching and Updating your Computer

Time to wake up, it is the second Tuesday morning of the month, do you know where your monthly Microsoft patches are? Is your computer all up-to-date? What about all the computers in the office; do they all have the most current patches applied? What is a patch, anyway?

Modern computer applications and Operating Systems are so complex these days that it is not uncommon for the developer of that application or program to find a way to make the application better (including to make it more secure) after it has been released, or sold, to the public. This means there has to be a way of getting that change to the public, a way for them to update the application, improving its functionality or security.

The way for this update to take place is through the issuance of a patch. The developer of the software will make an announcement that a patch is on the way, and for all those who use that application, they should go to the developer's website and download that patch.

Managing all the patches for all the applications and Operating Systems on an entire network can be a difficult task. It is the responsibility of the administrator to ensure that all systems are updated, as one system without current security patches presents a vulnerability to the entire organization.

On the Operating System side, Microsoft has what has become known as "Patch Tuesday". Microsoft found that issuing patches and making them available to customers was not effective enough. Customers knew the patches existed, but did not go online to download them. Then next step was to send these patches directly to computers, making it easier for customers to receive the proper patches.

Through the use of Automatic Updates, Microsoft's customers will receive security patches on the second Tuesday of each month. This makes it much easier on administrators to ensure that Microsoft systems are updated. This strategy, however, is not without limitations and downsides.

Having security patches issued monthly allows for those who exploit computers to know the schedule of release for potential defenses against exploits. Attackers will wait to see if the current patches impact their attacks in any way, and if so will know how much time until the next patch is released. It is not uncommon, therefore, to see new attacks on Microsoft products released on the Wednesday following Patch Tuesday.

Another potential issue is that often these patches on Tuesday will require an automatic restart of the computer. Having millions of computers restarting in a short window can impact other services. The online VoIP (voice over IP) service Skype experienced a major outage for almost two days in the Fall of 2007. The outage was said to have been partially triggered by the number of computers restarting from the Automatic Updates, and then trying to authenticate and log onto the Skype network upon restart. The volume

of authentications at the same time was listed as the event that took the service offline. You can read the notice from Skype [here](#).

Although there are many different methods of patching your systems, there are some important suggestions to make the patching process more effective on your systems. These key suggestions include the following:

- Backup your systems prior to installing a new patch. In the event there is a problem during the installation, or other negative impact on the system, the backup is critical.
- Test any patches you are going to install on a test platform, prior to installing on an operational system. Sometimes a patch can have unintended consequences, especially if there are many different (or custom) applications on a system, so testing ahead of time is strongly suggested.
- Create a database that lists the current patches on all systems. This will allow you to quickly reference and see the patch status of all your systems. Some systems may not need the same patches as some others, even if they are the same base Operating System, depending on the purpose of the system itself.
- Ensure you have a roll-back, or uninstall method if the patch is not required, or for any other reason, needs to be removed from the system. Some patches include uninstall options, others do not. This is directly tied to your backup and testing method of patching.

Following these suggestions the implementation of patches in your organization can run more smoothly, and will allow you to manage this aspect of running and securing the network more efficiently.

*Warren Peterson is the President and co-founder of Security Certified Program,
www.SecurityCertified.Net*