

Windows Security Patching and FNAL Computers

Automated and Manual Procedures for Windows Computers

Fermi Domain Computers

Computers in the Fermi Windows Domain are covered by a 2 tier infrastructure for security patches:

- Tier 1 is the responsibility of the OU manager. At this level patching is done via Patchlink, SMS, Windows Update, or another product
- Tier 2 is a Microsoft Software Update Server. Patches that have been declared critical by the Computer Security Team are enabled and mandatory for all machines in the Fermi domain

If a domain computer is properly patched at the Tier 1 level then Tier 2 settings have **NO** affect on the computer. If a domain computer isn't patched properly then the Tier 2 service will download patches to the computer, apply them, and reboot the computer if necessary.

Remember: Machines missing critical patches can lose network access!

Non-Fermi Domain Computers

Computers that are not in the Fermi Windows Domain are the responsibility of the designated system administrator. These systems can participate in the Tier 2 service by making a small registry change:

```
REGEDIT4
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]  
"RescheduleWaitTime"=dword:00000005  
"NoAutoRebootWithLoggedOnUsers"=dword:00000000  
"NoAutoUpdate"=dword:00000000  
"AUOptions"=dword:00000004  
"ScheduledInstallDay"=dword:00000000  
"ScheduledInstallTime"=dword:00000006  
"UseWUServer"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]  
"WUServer"="http://sus.fnal.gov/"  
"WUStatusServer"="http://sus.fnal.gov/"
```

This file is available at: <http://www-win2k.fnal.gov/pub/SUS>.

How to Patch Your System

Administrative access to the machine is required to install patches!

Windows Update

On systems where it is available Windows Update is a reliable way to apply Microsoft supplied patches to a computer. Network connectivity is required

Manual

Patches can be downloaded from Microsoft or PSeeKits and installed. Individual patches and rollup scripts are available. These can be written to a CD or USB drive to patch machines that are not on the network

- <http://pseekits.fnal.gov/fermi-rollup>
- `\\pseekits\fermi-rollup`

Checking Patches

There are four recommended ways to check if your system has the correct patches: Windows Update, MBSA(Microsoft Baseline Security Analyzer), Registry, and Add/Remove Programs Control Panel.

Windows Update

You must have administrative access to the system! Things to remember about Windows Update:

- Windows Update checks for all OS patches – not just security related items
- Only patches that Windows Updates determines are necessary are available
- Care must be exercised to not apply patches that aren't necessary

MBSA

You MUST have administrator access to the system! This is a free download from Microsoft and comes in either a GUI or command line tool. A version of the command line tool set to check Fermi domain systems is available at:

`\\pseekits\desktoptools\hfnetchk\chk-patch.cmd`

Registry

The brave can poke around the registry and get a list of patches applied to their system by looking at `HKLM\SOFTWARE\Microsoft\Updates`. You'll see a list of Knowledge Base numbers for the installed patches. The installed patches must be compared to what patches are required for the particular OS.

Checking Patches – Add/Remove

In this control panel applet the MS KB numbers for patches that are installed are shown. In either case the installed patches must be compared to what patches are required for this particular OS.

Questions???

If you have questions about patching systems please contact the Windows Policy Committee (winpol@fnal.gov) or Computer Security (computer_security@fnal.gov)