



FNAL System Patching Design

Jack Schmidt, Al Lilianstrom, Andy Romero, Troy Dawson, Connie Sieh
(Fermi National Accelerator Laboratory)

Introduction

FNAL has over 5000 PCs running either Linux or Windows software. Protecting these systems efficiently against the latest vulnerabilities that arise has prompted FNAL to take a more central approach to patching systems.

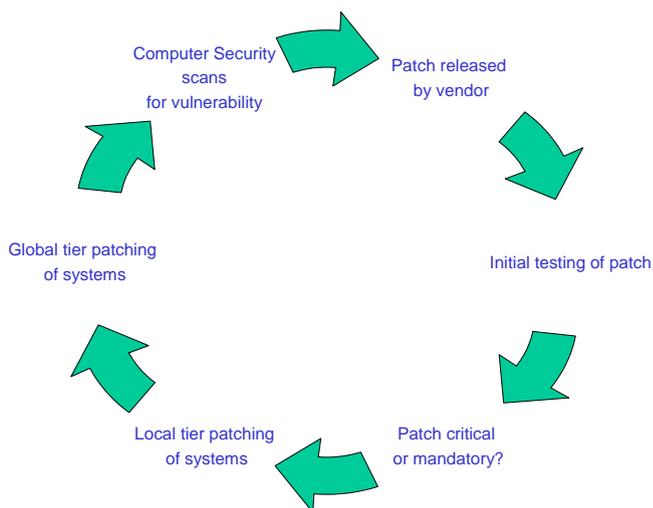
Due to different levels of existing support infrastructures, the patching solution for linux systems differs from that of windows systems. In either case, systems are checked for vulnerabilities by Computer Security using the Nessus tool.

Windows Patching Overview

Until fall of 2003, Fermilab Windows administrators used a variety of methods to apply software patches to address security flaws. Many of these methods were slow, unreliable and labor intensive. Due to the recent onslaught of vulnerabilities, the CSExec asked the Windows Policy Committee to design a patching solution that provides critical updates to systems in a timely manner. The solution had to make use of the existing Active Directory structure but also be available for non-domain systems.

The working group met and reviewed existing patching methods across the lab, identifying positive and negative issues with each solution.

Windows Patching Cycle



Patching Solution Design

Based on the working group study, a two-tiered system for patch deployment; Local Tier and Lab-wide Tier. Computer Security along with the Windows Policy Committee define patches that are required by windows systems present on the Fermilab network. Patch deployment is based on level of criticality, existing infrastructure prevention (ie site NetBIOS blocks, VPN usage, etc) and threat assessment.

Patch Approval Process

When a critical patch is released to address a security flaw, Computer Security with the advice of the Windows Policy Committee decides whether or not the patch will be declared to be *mandatory*. Patches that address flaws which allow remotely initiated compromises will almost always be declared to be mandatory. Patches are initially tested by the Computing Division to verify basic compatibility. Once a patch is approved for deployment two things happen, (1) local administrators must deploy the patch using their Local Tier systems and (2) Computer Security will specify a date, on which deployment from the Labwide Tier will be enabled.

Note: At any time during the testing, local system administrators can choose to deploy the patch to their systems using their Local Tier.

Local Tier

Each division and section at Fermilab configures their systems (software and hardware) in order to meet their specific requirements. Because system configurations are not uniform, patching requirements are not uniform. Each major local support group manages their part of the Local Tier of the patch deployment system.

Local Tier Implementation

Local support groups can implement and maintain their own Local Tier system. If local support groups decide to do this, they can use any product or combination of products; the only requirements are: *the system must work, the system must not violate Computer Security Policy and the system must not be disruptive.*

Local support groups also have the option of using the Site Local Tier server provided by the Computing Division.

Labwide Tier

Patches deemed mandatory, require a redundant level of patch protection. For this reason a lab-wide patch deployment system was implemented. The Lab-wide Tier is centrally managed by the Computing Division with oversight provided by Fermilab Computer Security. The Labwide Tier automatically deploys mandatory patches to those systems which were missed by the Local Tier at the end of the deployment lifecycle.

Lab-wide Tier Implementation

The Labwide Tier uses Microsoft Software Update Services (SUS). The Fermilab implementation of Microsoft SUS has two main components: a single SUS Update Server and the Automatic Update Service. The SUS Update Server is a Windows 2000 server running IIS and Update Server software from Microsoft. The Automatic Update Service runs on Windows 2003, Windows 2000 and Windows XP client computers. The Automatic Update service on client computers in the FERMI domain are configured using a domain level group policy object (GPO). The domain level SUS GPO will automatically set several client parameters; one of the parameters points client systems to the Fermilab SUS Update Server. Sometime after a client system is configured by the domain level SUS GPO, the set of patches installed on the client will be compared with the set of mandatory patches; any missing mandatory patches will be deployed to the client. Note that, non FERMI domain systems can be manually configured to point to the Fermilab SUS Update Server.

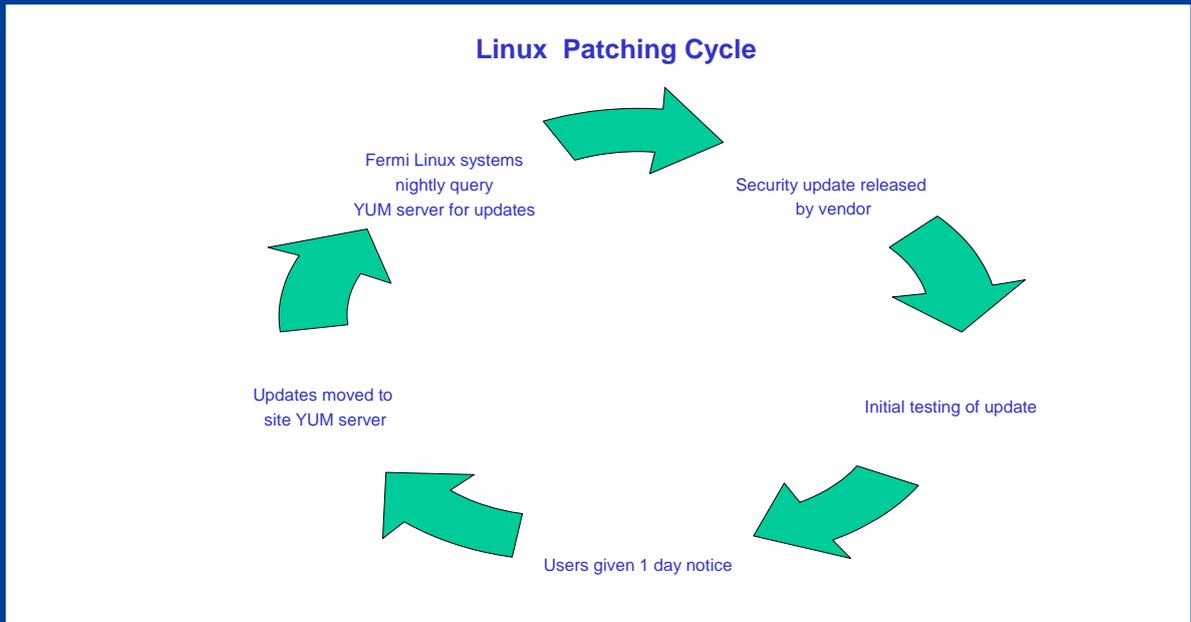
Critical Patch Exemptions

It is possible that patch testing will show that there is a conflict between a mandatory patch and the operation of a system which provides an important service (for example: payroll, beam control). For each conflicting patch, the administrator of such a system requests an exemption with Computer security.



FNAL System Patching Design

Jack Schmidt, Al Lilianstrom, Andy Romero, Troy Dawson, Connie Sieh
(Fermi National Accelerator Laboratory)



Linux Patching Overview

1999 Gave users optional use of auto patching via autoprpm. Next release it was installed by default.

2000 Kerberized linux is required to use the FNAL network. Increase in users of Fermi Linux!

2002 Switched from autoprpm to YUM. YUM (Yellowdog Update Manager) is an automatic updater and package installer/remover for linux systems.

2004 Scientific Linux released. Site customizations built on Scientific Linux are automatically patched.

FNAL currently provides security errata for 7.3.x, LTS 3.0.x, SL 3.0.x

Patch Rollout Steps

Vendor releases security updates.

Patches are reviewed by the Linux Support team and tested on basic systems.

Reviewed and tested updates are moved to the "YUM" distribution server security update area.

Each night YUM checks to see if there are new security updates that are needed to be installed. The Fermi Linux Support team will make announcements via the linux-users mailing list about the availability of a security update.

Users are given 1 day notice before the update is moved to the "YUM" server.

fermilinux



Fermi Linux Users

