NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

# Procedures for Handling Security Patches

Timely patching is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is the most common mistake made by IT professionals.

New patches are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches.

**Vulnerabilities** are weaknesses in software that can be exploited by a malicious entity to gain greater access and/or permission than it is authorized to have on a computer.

Not all vulnerabilities have related patches; thus, system administrators must not only be aware of vulnerabilities and patches, but also mitigate “unpatched” vulnerabilities through other methods (e.g. workarounds, firewalls, and router access control lists).

Organizations have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches.

This document provides principles and methodologies for accomplishing this.

# The Patch Management Process

Patch management is a circular process and must be ongoing.

- **Detect**. Use **tools to scan your systems for missing security patches**. The detection should be automated and will trigger the patch management process.

- **Assess**. If necessary updates are not installed, **determine the severity of the issue(s) addressed by the patch and the mitigating factors** that may influence your decision. By balancing the severity of the issue and mitigating factors, you can determine if the vulnerabilities are a threat to your current environment.

- **Acquire**. If the vulnerability is not addressed by the security measures already in place, download the patch for testing.

- **Test**. Install the patch on a test system to verify the ramifications of the update against your production configuration.

- **Deploy**. Deploy the patch to production computers. Make sure your applications are not affected. Employ your rollback or backup restore plan if needed.

- **Maintain**. Subscribe to notifications that alert you to vulnerabilities as they are reported.

**Begin the patch management process again.**

# Patch and Vulnerability Group

One of several possible techniques is through the creation of a patch and vulnerability group (PVG). This group would facilitate the identification and distribution of patches within the organization.

The personnel involved should have broad knowledge of patches, systems administration, and computer vulnerabilities.

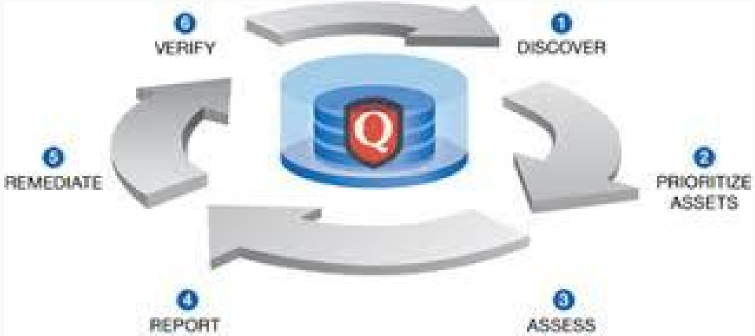
- ❏ Creating an organizational hardware and software inventory.
- ❏ Identifying newly discovered vulnerabilities and security patches.
- ❏ Prioritizing patch application.
- ❏ Creating an organization-specific patch database.
- ❏ Testing patches for functionality and security.
- ❏ Distributing patch and vulnerability information to local administrators.
- ❏ Verifying patch installation through network and host vulnerability scanning.
- ❏ Training system administrators in the use of vulnerability databases.
- ❏ Deploying patches automatically.
- ❏ Configure Automatic Update of Applications.

If organizations use the PVG approach, **this would not diminish the responsibility of all systems administrators to patch the systems under their control.**

**Each systems administrator would.**

- ★ Apply patches identified by the PVG.
- ★ Test patches on the specific target systems.
- ★ Identify patches and vulnerabilities associated with software not monitored by the PVG.

The duties of the PVG will be to **support local administrators in finding and fixing vulnerabilities** in the organization’s software.



## Create and Maintain an Organizational Hardware and Software Inventory.

- **Create a database containing the hardware equipment and software packages and version numbers of those packages** most used within the organization.

- Once the organizational hardware and software inventory has been created, it will be necessary to **maintain this inventory.**

- **The maintenance of the inventory** will require the PVG to work closely with system administrators so that the inventory is updated in a timely manner when a system is installed or upgraded

# Identify Newly Discovered Vulnerabilities and Security Patches.

- **The PVG is responsible for monitoring security sources for vulnerabilities and patches** that correspond to the software within the PVG's organizational software inventory.
- **When a vulnerability has no satisfactory patch, the PVG will present alternative risk mitigation approaches to IT management** and support the management decision by testing, documenting, and coordination implementation with the appropriate system or network administrators.

# Prioritize Patch Application.

- **The PVG must prioritize the set of known patches** and provide advice to local administrators on the criticality of each patch.
- A distinction must be made between servers and end-user systems when making patching recommendations because **often it is more important to patch servers before end-user systems** and to more thoroughly patch the servers.

# Create an Organization Specific Patch Database.

- **The PVG should create a database of information on the patches** that apply to the organization. Ideally, the database should contain the actual patches and instructions on installing those patches.

- A copy of each patch may be needed in situations when the Internet may not be accessible or the vendor’s website may have been compromised.

# Conduct Generic Testing of Patches.

- If an organization uses standardized host configurations, the PVG will be able to test patches on those configurations. This will **avoid the need for redundant testing by each local administrator.**

- The PVG should also work closely with local administrators to test patches on important servers systems.

# Distribute Patch and Vulnerability Information to Local Administrators.

The PVG is responsible for informing local administrators about patches that correspond to software packages included on the organizational software inventory.

## Verify Patch Installation Through Network and Host Vulnerability Scanning.

- The PVG should **perform periodic network and host vulnerability scanning** to identify systems that have not been patched.

- The PVG should be aware that network and host vulnerability scanners do not check for every known vulnerability and thus cannot be relied on as a sole source of vulnerability information.

- The PVG **should inform local administrators** that they are performing such periodic scanning.

# Train System Administrators in the Use of Vulnerability Databases.

- It is essential that **local administrators have some knowledge of how to identify new patches and vulnerabilities.** By providing them with such knowledge, we create a second line of defense in our patching process.
- **Local administrators should be trained by the PVG** on the various vulnerability and patching resources

# Perform Automatic Deployment of Patches (When Applicable).

Some organizations with largely homogeneous computing platforms can use automated distributed patch deployment services.

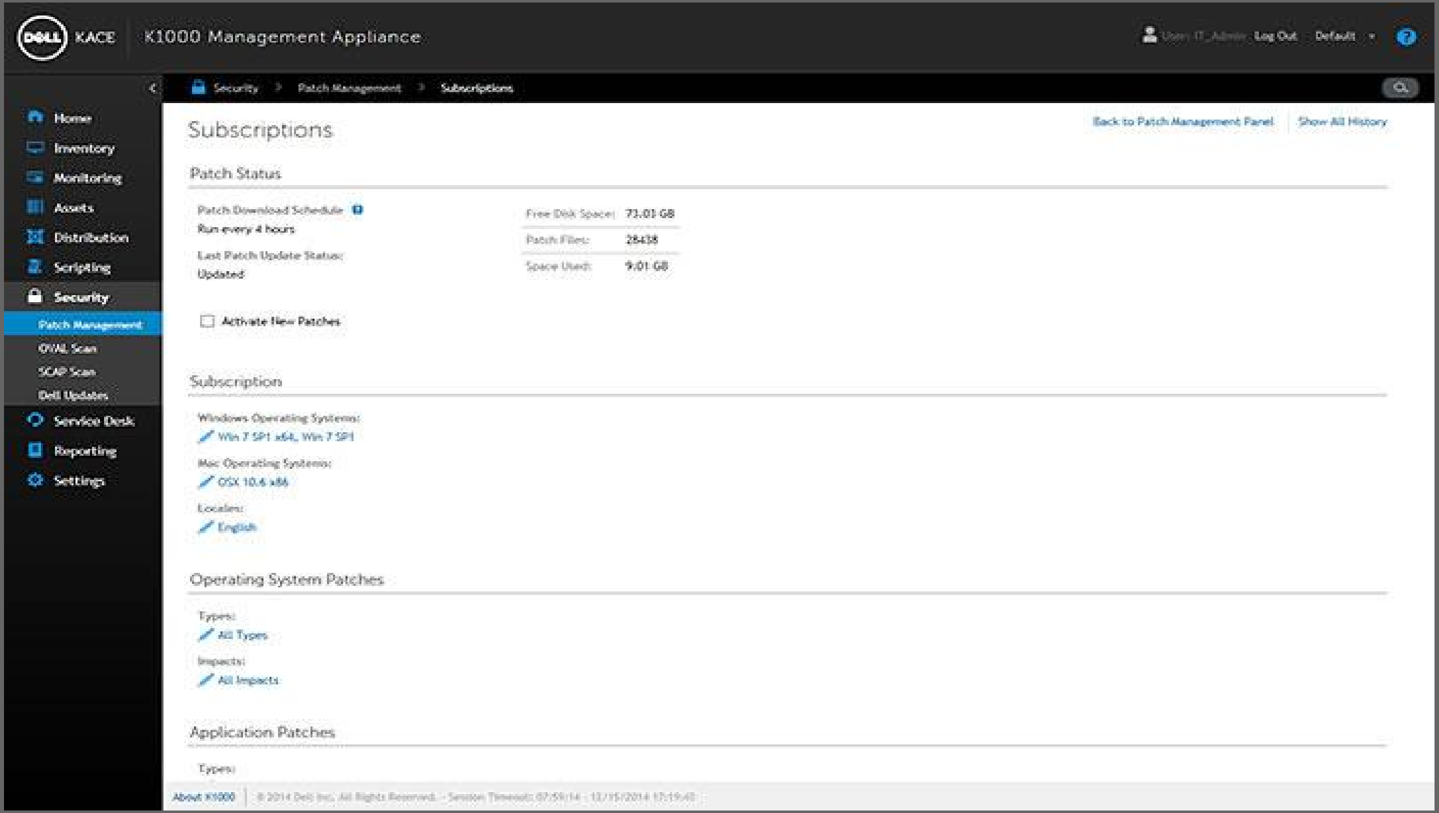
Thus, an administrator from a single console can update hundreds or even thousands of systems. This job function could be effectively performed by the PVG. If not, the **PVG should work very closely with the administrator** in charge of the patch deployment system to ensure that all applicable patches are applied.

# Configure Automatic Update of Applications (When Applicable)

Many newer applications provide a feature whereby the application check against the vendor’s Website for updates.

The most common forums for monitoring the release of patches and identification of vulnerabilities are as follows

- Vendor websites and mailing lists
- Third-party websites
- Third-party mailing lists and newsgroups
- Vulnerability scanners
- Vulnerability databases
- Other notification tools
- Windows Update.



## Subscriptions

### Patch Status

Patch Download Schedule
Run every 4 hours

Last Patch Update Status:
Updated

| | |
|---|---|
| Free Disk Space: | 73.01 GB |
| Patch Files: | 28438 |
| Space Used: | 9.01 GB |

□ Activate New Patches

### Subscription

Windows Operating Systems:
Win 7 SP1 x64, Win 7 SP1

Mac Operating Systems:
OSX 10.6 x86

Locales:
English

### Operating System Patches

Types:
All Types

Impacts:
All Impacts

### Application Patches

Types:

© 2014 Dell Inc. All Rights Reserved. - Session Timeout: 07:59:14 - 12/15/2014 17:19:40

https://www.youtube.com/watch?v=_syM-nb7Lgo

# Top Patch Management Software Products

http://www.capterra.com/patch-management-software/

# DEMO

http://systems.demo.solarwinds.com/Orion/DPA/Summary.aspx

**NIST Special Publication 800-42, Guidelines on Network Security Testing, offers advice on techniques for vulnerability scanning.**