DEFINITION

patch management

Posted by: Margaret Rouse WhatIs.com

Contributor(s): Brien Posey

Patch management is an area of systems management that involves acquiring, testing and installing multiple patches, or code changes, to an administered computer system. Patch management tasks include maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required. Several products are available to automate patch management tasks, including RingMaster Software's APM, ManageEngine's Desktop Central and SolarWinds Patch Manager.

Why is patch management important?

Patch management is important because patches help to maintain the health and security of the systems that are being patched. Additionally, patches are sometimes used to bring software up to date so that it will work with the latest hardware.

How does patch management work?

Patch management works differently depending on whether a patch is being applied to a stand-alone system or is being applied to systems on a corporate network. In the case of a stand-alone system, the operating system and the applications on that system will periodically perform an automatic check to see if any patches are available. If new patches are found to exist, the patches will typically be downloaded and installed automatically.

Patch management tends to work differently in a corporate environment, because organizations generally try to maintain software version consistency across their computers. As such, organizations usually perform centralized patch management rather than allowing each computer to download its own patches.

Centralized patch management uses a centralized patch management server that downloads patches on behalf of the organization and distributes those patches to the computers on the organization's network in accordance with the organization's patch management policy.

A centralized patch management server does more than just automate patch management. It also gives the organization a degree of control over the patch management process. For example, if a particular patch is determined to be problematic, then the organization can configure its patch management policy to prevent that particular patch from being deployed.

Another advantage to performing centralized patch management is that doing so helps to conserve internet bandwidth. It makes little sense from a bandwidth perspective to allow every computer in the entire organization to download the exact same patch. Instead, the centralized patch management server can download the patch and then distribute it to all the computers within the organization. This means that the patch only must be downloaded once, rather than downloading a separate copy for every computer.

Although many organizations handle patch management on their own, some managed service providers perform patch management in conjunction with the other network management services that they provide to their clients.

Benefits of patch management

Most major software companies periodically release patches for their products. These patches can serve any of three primary purposes.

First, patches are often used to address security vulnerabilities. If a software vendor discovers that there is a security risk associated with its product, it will commonly issue a patch to address that risk. It is important that organizations apply security patches as quickly as possible, because hackers and malware authors know about the security vulnerabilities that a patch is designed to correct, and actively look for unpatched systems.

A second reason why software companies commonly release patches is to fix bugs that have been discovered in their software. Applying such patches can improve software stability, while also getting rid of annoying problems.

Third, software companies occasionally release patches as a way of introducing new features. Feature updates are becoming much more common than they once were as a result of the transition to subscription-based software licensing.

Common problems with patch management

The most common problem associated with the patch management process is that of a buggy patch. Occasionally, a patch will introduce problems that did not previously exist. These problems may show up in the product that is being patched, or the problems may manifest themselves elsewhere if other software has a dependency relationship with the software that was recently patched.

Because patches can sometimes introduce problems into a system that was previously working correctly, it is important for administrators to test patches prior to deploying them on an organizationwide basis.

Another common problem associated with patch management is that disconnected systems may not receive patches in a timely manner. If a mobile user rarely connects to the corporate network for instance, then that user's device may go for long periods of time without being patched. In such cases, it may be better to configure the device for stand-alone patch management rather than relying on centralized patch management.

Patch management life cycle

When a new patch is released, an organization should test the patch before deploying it on an organizationwide basis. The IT department may initially perform some basic tests inside of a sandbox environment. This keeps any problems with the patch from impacting production systems.

If no obvious problems are discovered during sandbox testing, then the IT department may perform a pilot deployment. A pilot deployment involves deploying the patches to a limited number of production systems to verify that the patch works properly in a production environment. After a period of time, the patch is deployed on an organizationwide basis.

Occasionally, the IT department may need to remove a patch that has been applied to production systems. This can happen if the patches are found to cause problems, but there are other reasons for removing a patch. A patch might be removed, for example, if a software vendor releases a new patch that cannot be put into place while the previous patch remains on the system. In such a case, the new patch is said to supersede the previous patch.

Examples of patch management

Microsoft often provides patches to its Windows operating systems and to other products such as Office 365. These patches are normally released on a scheduled basis, on a day that has come to be known as Patch Tuesday.

Margaret Rouse asks:

How does your company handle patch management for
enterprise applications?

Join the Discussion

Stand-alone systems rely on Windows Update to automatically download and deploy any available patches. In business environments, however, it is much more common to use Windows Server Update Services to manage and deploy Microsoft patches. The Windows Server Update Services, which are commonly referred to as WSUS, are included with Windows Server and specifically designed to centralize patch management. However, there are numerous third-party products that are also able to download, manage and deploy Microsoft patches.

This was last updated in January 2020

Next Steps

See how patch management software works to keep your company protected and compliant, and learn about the many benefits of patch management tools.

Read the seven tips to evaluating patch management tools, and then see which patch management vendor best fits your company's needs. For more information about each product, check out this patch management vendor roundup.

Continue Reading About patch management

- 5 enterprise patch management best practices
- Complexity requires new cloud-based patch management strategies
- Optimize application deployments with this expert advice from 2019
- How to automate patch management in Windows
- Patch management: How to prioritize an underserved vulnerability

Related Terms

application performance monitoring (APM)

Application performance monitoring (APM) is the collection of tools and processes designed to help information technology (IT) ... See complete definition ℹ

remote desktop protocol (RDP)

Remote desktop protocol (RDP) is a secure network communications protocol from Microsoft. See complete definition ℹ

unified endpoint management (UEM)

Unified endpoint management (UEM) is an approach to securing and controlling desktop computers, laptops, smartphones and tablets ... See complete definition ℹ

Dig Deeper on Windows 10 security and management

5 WSUS alternatives for patch management

How to plan an SAP S/4HANA brownfield migration

By: Brad Hiquet

3 crucial Linux patch management best practices for IT

By: Brien Posey

5 RMM tools MSPs can use to bolster client IT infrastructure

By: Esther Shein

Join the conversation

1 comment

Share your comment

☑ Send me notifications when other members comment.

Create Username and Add My Comment

Oldest ▼

[-] Margaret Rouse

- 21 Sep 2005 11:45 AM

How does your company handle patch management for your enterprise applications?

Reply

VIRTUAL DESKTOP WINDOWS SERVER

SearchVirtualDesktop

How to troubleshoot a VMware Horizon black screen

One of the most common issues with VMware Horizon virtual desktops is a black screen displaying and crashing the desktop, so IT ...

Running GPU passthrough for a virtual desktop with Hyper-V

Any IT admin knows that desktop performance must be high quality to provide quality UX, and in some cases, admins may need to ...

About Us Meet The Editors Contact Us Advertisers Business Partners Media Kit Corporate Site

Contributors Reprints Answers Definitions E-Products Events Features

Guides Opinions Photo Stories Quizzes Tips Tutorials Videos

Privacy Policy

Do Not Sell My Personal Info