ManageEngine

Introduction

To reach business targets, enterprises must formulate an effective IT strategy. A core part of this strategy depends on the configuration management you have in place as part of your IT security policy.

Your IT security policy must control day-to-day operations, monitor system performance, provide accounting and reporting functions, address risks and failure management, and reduce downtime. The process of patch management is a fundamental component of configuration management for your endpoints.

Patch management is the sequential process of addressing security need gaps by keeping network computers updated. It involves:

- Inventorying the network OSes and applications
- Discovering network vulnerabilities due to missing patches
- Planning a risk assessment strategy
- Implementing a critical patch-first approach
- Testing for stability before distribution
- Aligning patch policies with software vendors' release models
- Deploying patches based on the update window

Patch management influences the configuration policies for servers and workstations, helps document network health periodically, and keeps network security up to date. Having a risk assessment strategy ensures the business continuity of servers and client machines. A good patch management process that utilizes an automation process and a regular schedule for applying patches is vital for a successful risk assessment strategy.

Let us look at some patch management best practices that ease IT administration and management.

PATCH MANAGEMENT BEST PRACTICES

A handy guide for a proactive network security

ManageEngine Patch Manager Plus

ManageEngine

Patch management best practices for 2020

1. Automate patch management — discover missing patches and deploy them

Manual patching is tedious, and often critical security patches are not rolled out efficiently. An automated patching tool that maintains a database of latest updates provides a better approach. Scheduling regular scans, downloading missing patches from vendor websites, updating the patch database, and defining deployment configurations should all be capabilities your automated patch management solution should offer. With automated patch management, administrators can schedule seamless patch distribution, regardless of the enterprise's size and without user intervention. This reduces the workload of the administrators, resulting in higher efficiency and productivity.

2. Detect vulnerabilities quickly, apply a "Critical Updates First" approach

Once a vulnerability occurs in an application, an exploit by cybercriminals looking to take advantage of it is likely on the way. A best practice of risk assessment in the patching process is to detect critical missing patches right away and alert users.

If you choose to automate the patching process, deployment will be rolled out quickly to reduce the impact of vulnerability on business operations. A best practice for all other important and non-security updates is to deploy during off-hours or during a scheduled maintenance window.

A good patch management strategy should include risk analysis and mitigation strategies, an automated process, and a defined schedule for applying patches. It should also take into account the importance of business applications, and keep a close eye on these applications. Whenever patches and hotfixes are released by vendors for these business-critical applications, they should be applied quickly to your network.

A computer's vulnerability is defined based on the number of missing patches. Non-critical updates on less vulnerable systems can be performed on a regularly scheduled maintenance window.

3. Deploy all business-critical applications, leave out none

Vendors like Microsoft provide resourceful applications for office purposes. While it is critical to patch these on a regular basis, patching non-Microsoft applications is equally important, and should be part of your patch management strategy. Applications like Adobe Flash, Google Chrome, Oracle Java, Mozilla, QuickTime, WinZip, FaceTime, and Teamviewer are all favorite targets for hackers.

Not all vendors provide frequent security updates. Adobe and Google Chrome release fixes/enhancements on "Microsoft Patch Tuesday," which occurs on the second Tuesday of every month. Java and Mozilla occasionally release security updates, and other vendors release security patches only when a vulnerability is exposed.

It is important to ensure the patching solution you use covers all applications used in the network, including third-party applications.

4. Know your network health status

- Keep track of important missing patches, computer vulnerabilities due to missing patches, failed patches, etc.
- Maintain an inventory of production systems, types of OSes, roaming computers, remote office machines under IP scope management, etc.
- Manage 'bring your own device'(BYOD) components, including laptops used for work that aren't company-owned.
- When new computers are added to your network, make sure they're covered under automated patching.
- Be aware of certain patches that shouldn't be deployed in your network because they can prevent other components from operating efficiently. Some versions of Java, for example.
- In case of a demilitarized zone (DMZ), also known as air-gap network, patches should be posted to an intranet server and distributed to clients for installation.

5. Keep your servers up to date

Servers are critical and need to be operational to ensure optimal productivity. Because of how quickly cyberattacks can spread through networks, if a vulnerable server is infected, the connected client machines are then vulnerable to also falling victim to the attack. Servers are also prone to exploitation when communicating with remotely connected users.
You can minimize server downtime by installing updates and patches during a standard maintenance window and using a backup server.

Continuously assess servers to determine if they have new or additional patch requirements. To keep up with the patch compliance status, automate patching of the critical/vulnerable server machine in the maintenance window.

6. Upgrade OSes to the latest version

Issued every spring (in April) and fall (in October), Windows OS updates typically provide many security features. However, when Microsoft feels an OS has reached the end of its useful life, it will announce End-of-Life (EOL) product life cycle details and will no longer release updates or product enhancements for that OS version beyond the designated EOL date.

Users of older Windows OS, especially those no longer covered through End of Support policies, might not receive the latest security fixes, leaving those systems vulnerable to exploits. The ransomware WannaCry that wreaked havoc in May 2017 targeted a known vulnerability in unpatched Windows machines. Apple also releases regular updates for macOS that improve usability and security features. For all OSes, it's best to upgrade to the latest version.

7. Evaluate patches in a test environment before distributing

In a phased approach to patch deployment in large networks, a crucial step when a new set of patches is available is to evaluate them in a test environment.

The test environment should mirror your network, containing the same types of OSes and applications used in production. Testing patches before deploying them helps ensure they're stable enough to be deployed. After successful deployment to the test machines, this process can be replicated throughout the rest of the enterprise.

8. Schedule at least two deployments each week

Security patches are released by Microsoft and Adobe during the second week of each month, and non-security patches are released during the fourth week. Any intermediate release of patches is in the form of bug fixes, security updates for zero day vulnerability, etc.

When should you apply patches? A best practice for enterprises is to schedule a minimum of two deployments every week. Your network should ideally consist of test machines, less critical production machines, more critical production machines/users' machines, less critical servers, and data-critical servers. The order of patch deployments should be:

- Test machines for stability testing
- Less critical computers
- More critical computers during a different patching interval from the less critical ones
- Less critical servers
- More critical data servers - again at a different patching interval

Again, as noted earlier, if there are patches for zero-day vulnerabilities, they need to deployed right away. This way, you can ensure that the network is not open to exploitation or left unpatched for a long time.

9. Create multiple configurations based on business requirements

You can create custom groups based on domains, OSes, hardware, presence of certain applications, users (local or remote office/roaming), etc. This helps you establish configuration policies tailor-made to each group's requirements, and it enables you to easily track deployments too.

You can create multiple configurations including:

- Download and deployment after Patch Tuesday
- Time of scan and download of missing patches (a best practice is doing this daily during set, non-business hours, or during the weekend)
- Type of applications to be deployed, such as Microsoft updates, Adobe updates, security updates, roll-ups, service packs, and anti-virus definitions
- Time of auto-deployment
- Reboot scheduling to ensure the process does not impact work hours

10. Re-attempt failed patches

Patches can fail during retrieval from a vendor website
or when being installed. You need to figure out why the patches failed and troubleshoot accordingly. Ultimately, you will need to modify the configuration so the patches are deployed successfully.

11. Generate detailed patch summary reports

IT reports are important for security auditing. You can generate detailed patch summary reports for successful and failed deployments, date of updating, version of application updated, etc. Tracking the patch summary is essential in risk assessment and helps ensure vulnerabilities are addressed.

12. Cover patch management in a heterogenous environment

Windows machines constitute 75% of the total global OS market share, while macOS constitutes 12%, Linux constitutes 1.6%, and approximately 10% is distributed among other OSes. The adoption of macOS in enterprises has increased in recent years.

If your network runs on Windows, Mac, and Linux computers, you will need to fetch different versions of patches from different websites. This is a tedious process if you are not using a patching solution that addresses all OS requirements.

The patch manager you select must automatically be able to inventory the OS of each computer as well as detect and deploy the required updates.

Conclusion

This document extensively addresses best practices that can reduce your patch management workload.

Choosing the patching solution that works best for your organization involves evaluating several factors. For example, is agent-based or agentless best? Agent-based patching software is more efficient in reducing patch failures, plus you can deploy to remote users more easily.

Also, a point product or configuration management software?
Is patching in your organization a dedicated task with allocated personnel? If so, you'll want to go with a point product. If you'd like to manage multiple administrative tasks like remote troubleshooting, software distribution, and patch management, then you need configuration management software.

Choose a complete patching solution—one that accommodates all your patching requirements, including all OSes and applications utilized in your network, as well as scanning, detecting, and downloading and deploying capabilities that require no manual intervention. Patch management is no easy ask, but with the help of best practices, you can secure your network big time.

ManageEngine, a division of Zoho Corp. Pvt. Ltd., offers a broad suite of enterprise IT management solutions for endpoint management and security, service and help desk, IT operations management, Active Directory and other security needs. Enterprises of all sizes rely on our real-time IT management tools to ensure IT-business alignment and optimal performance of their IT infrastructure, including networks, servers, applications, desktops and more.

ManageEngine solutions for patch management

ManageEngine
Patch Connect Plus

*A third-party patching solution for SCCM users for over 300 applications. Available as an **add-on patching tool to SCCM & as downloadable catalog files** that can be configured in your SCCM environment.*

Free Trial **Learn more**

ManageEngine
Patch Manager Plus

*An exclusive patching solution that completely automates the patching of **Windows, Mac, and Linux** applications as well as third-party applications. Available as both **on-premise and on-demand software**.*

Free Trial **Learn more**

ManageEngine
Vulnerability Manager Plus

*Assess vulnerabilities along with automated patch management for **timely risk reduction**. You can also manage **web server hardening**, **security configurations**, **and high-risk software audits** to reduce your attack surface.*

Free Trial **Learn more**

ManageEngine
Desktop Central

*A **unified endpoint management and security software** with patch management, software deployment, remote troubleshooting, mobile device management, inventory management, OS deployment & other capabilities.*

Free Trial **Learn more**

Endpoint Management & Security Solutions