

Patch Management Best Practices

Mark Nicolett, Ronni J. Colville

Patch management best practices operationalize the steps of the vulnerability management life cycle and require processes that span IT security and IT operations.

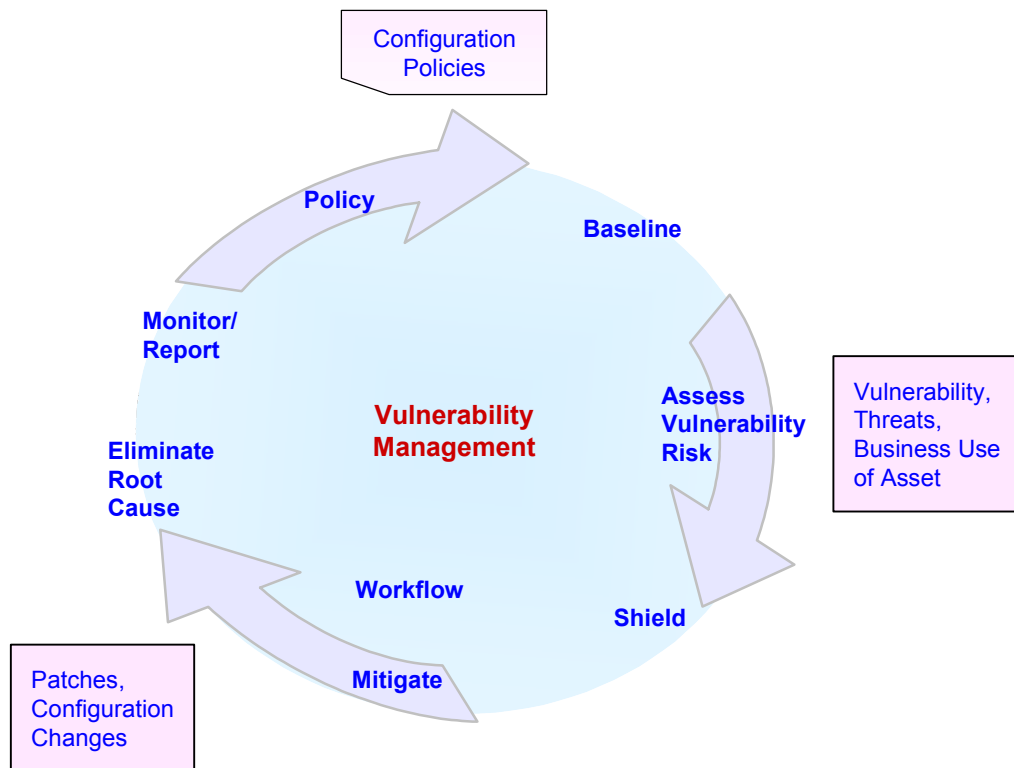
ANALYSIS

Patch management best practices are grounded in an assessment that balances the security and availability risk of a security breach with the cost, disruption and availability risk associated with the frequent and rapid deployment of software updates or system configuration changes. Best practices implement operational processes that support rapid change testing and deployment. The steps for patch deployment are almost identical to what is required for any system change — change assessment, change scheduling, quality assurance testing, packaging, distribution and installation — but there are some very important differences. System maintenance processes are designed to minimize disruption to business processes. The general approach is to bundle multiple system changes into large updates that are thoroughly tested and deployed on a quarterly, semiannual or annual schedule. Critical security patches, on the other hand, are small, frequent, high-priority changes that need to be rapidly installed on a large number of systems.

Enterprises have taken two approaches to patch management over the past four years. Some have taken a tactical approach addressing only the need at hand — deploy a patch to remediate a potential vulnerability. However, enterprises should treat patch management as just one part of an overall security and configuration strategy (see Figure 1). Organizations that have focused on the broader context of configuration management have used patch management as the impetus for a long-needed organizational shift. The shift brings together the security and IT operations organizations through a process that continually assesses both configuration-based and software-based vulnerabilities and provides remediation where appropriate and necessary with a foundation based on better standardization. Best practice requires the coordinated efforts of IT security and IT operations and drives process across both of them:

- *The Security Role* — The IT security organization drives the creation of a process that governs IT operations activity in response to the disclosure of a new vulnerability or the release of a critical security patch. The security organization is also responsible for monitoring for new vulnerabilities, evaluating risk and working with IT operations to determine the priority of a vulnerability-related patch or configuration change. Internal service-level agreements (SLAs) should be defined for all areas that are involved in the patch management process (IT security, network engineering, quality assurance [QA] testing, and the support groups for desktops, servers and applications). The SLAs define maximum time for completion of tasks such as QA testing and patch installation, based on a priority that is set via a risk assessment. The process needs to be sanctioned and supported by both IT and business management.
- *The IT Operations Role* — The IT operations team is responsible for maintaining the availability of the infrastructure overall and for implementing security patches and configuration changes. Within the operations team there are different groups responsible specifically for the configuration consistency of the network, servers and desktops, often not only with different teams but with different processes and automation as well. These groups establish policies and standards to be enforced against SLAs. Best-in-class organizations often supplement expertise and processes with tools to automate discovery, deployment and reporting (inclusive of patching).

Figure 1. Patch Management Within the Vulnerability Management Life Cycle



142266-2

Source: Gartner (August 2006)

Configuration Policy and Baselining

The first step in moving from a tactical to a more strategic approach is to establish standards that define settings for secure configurations. Once standards have been established, the next step includes discovering how systems are configured using security configuration management or discovery/inventory tools. These tools are either part of a configuration suite or provided as specialized security configuration management tools. Baselining also provides a foundation of information that can be used to form groups of systems that are similar. This information can be used to aid in risk assessment and to optimize QA testing and targeting for patch deployment.

Standard configurations that include security best practices support patch management at multiple levels. "System hardening" through security configuration management reduces the total number of vulnerabilities that are present in an IT environment, minimizing the number of systems that need to be patched. This effect is strongest in the server environment. Rapid and effective patch QA testing is possible when PCs and servers are deployed and maintained with standard configurations. QA testing is also more effective and availability issues are minimized because there is less uncertainty about the behavior of a patch when it is installed on production systems that have standard configurations.

Vulnerability Monitoring, Risk Assessment and Prioritization

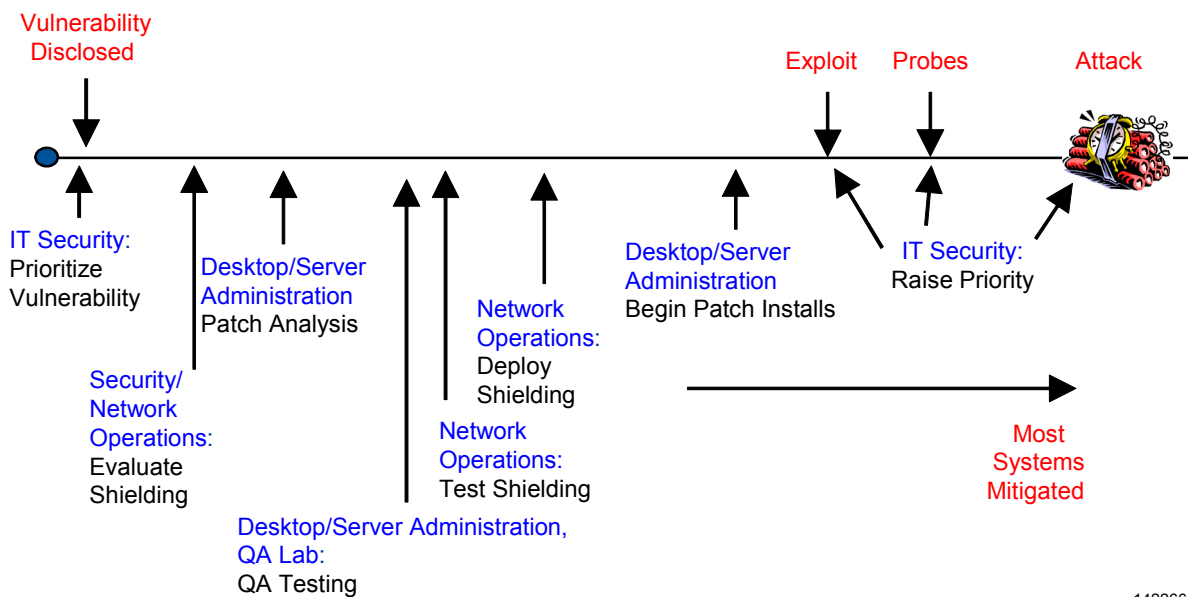
One group (the security organization in many companies) should be responsible for monitoring for new vulnerabilities, completing an initial risk assessment and assigning a mitigation priority.

This risk assessment should be based on information about the vulnerability, the current threat environment, general knowledge of the IT environment, and business use of vulnerable assets. Based on priority, the process needs to define the required mitigation speed (that is, the patch install speed or the implementation of compensating controls when business realities preclude patching by the required time). We believe the security group should be responsible for this task because as compared with IT operations, the IT security group is less subject to pressure by business areas to maintain system uptime at the expense of a needed security change. This task needs to be performed in a way that minimizes delay. For example, the group responsible for this task should be part of Microsoft's "Preview Thursday" so that it gets early information before "Vulnerability Tuesday." The group needs to keep up with all vendors' planned patch release schedules or subscribe to some service that does this for them.

Internal SLAs and Remediation/Patching Speed

Once the vulnerability is prioritized, the response by the rest of the organization to complete subsequent steps should be governed by internal SLAs (see Figure 2).

Figure 2. Patch Management Timeline



142266-2

Source: Gartner (August 2006)

Subsequent steps include evaluation, test and deployment of network-level blocking functions, and QA testing, scheduling and deployment of patches or security configuration changes. Best practice is to have specific SLAs for "QA test and install completion times" for each major system category. Priority and patching speed should be adjusted with changes to the external threat environment (that is, if the likelihood of an attack increases, the patch priority should increase).

Patching speed is a risk-based decision that needs to be made in the previous prioritization step. Many organizations have set goals for critical security patches for Windows systems based on the disclosure-to-attack time of major worms. Experience has shown that when an automated exploit targets a Windows vulnerability that is present on both Windows desktops and servers (that is, an operating system, common service or common component), the exploit can spread very rapidly across consumer PCs and then to corporate PCs and corporate Windows servers. As a consequence, many organizations have an overall goal to patch critical vulnerabilities on

Windows systems in a week or less. In general, patching is slower on all server platforms because of additional QA testing and uptime requirements. Many organizations that are able to patch a large number of Windows PCs in less than a week have at least some Windows servers that are not patched for a week or two (unless there is a clear indication or an expectation of an attack).

As a practical matter, patching speed will vary based on the use of the system. For example, standard Windows desktops that are in use only during office hours can be quickly QA-tested and then patched with a high level of automation. Some groups of PCs may take longer to patch. Examples are PCs with complex application stacks, PCs used in a clinical or production control setting, and laptops used by highly mobile workers. QA testing and update scheduling will take longer for an application or database server than it will for standard Windows desktops that are used only during office hours. Different patch management SLAs should be set for the major system classes that exist within an organization.

Database Management Systems and Linux and Unix Servers

Database management systems and Linux and Unix servers also require security configuration management and patching when there are critical vulnerabilities present on these systems. "Wormable" attacks are less common and less virulent on these platforms because there is not a large number of misconfigured Internet-connected systems to aid in rapid spread (as there is with consumer Windows desktops). As a consequence, many organizations do not apply security patches or configuration changes outside of the traditional quarterly or biannual maintenance schedule for these systems. However, there has been a growing number of targeted attacks against application and database servers that begin with the exploitation of a known vulnerability. For this reason, security configuration and patch management processes must be applied to these systems as well. Organizations should implement a process to prioritize critical security updates on these systems and to quickly remediate critical vulnerabilities.

Mitigation

Full automation of all patch management functions (patch analysis, packaging, targeting, distribution and install) is needed most in cases where patches must be installed frequently, very rapidly and on a very large number of systems. The automation need is greatest for Windows desktops, followed by Windows servers, and then Unix and Linux servers. Desktop support, Windows server administration and Unix/Linux administration groups are responsible for implementing patches and security configuration changes, and decisions about patch management automation need to be made in the context of the processes and tools (capabilities and limitations) that are currently in use by these organizations. Organizations should evaluate the security configuration and patch management capabilities of incumbent desktop configuration management and server configuration/provisioning tools, and they should also include security configuration and patch management requirements in RFPs for these technologies. In some cases it will make sense to augment existing operational tools with security configuration and patch management point solutions.

Many IT environments have systems with vulnerabilities that cannot be quickly remediated (see "Identifying and Solving Vulnerability Management Weak Spots" and "Finding and Solving Vulnerabilities in Embedded Operating Systems"). In cases where change window constraints, application compatibility issues or other conditions prevent the timely deployment of patches or security configuration changes, there should be investigation of additional blocking strategies. Examples include isolation of vulnerable servers on their own network segments and behind intrusion prevention technology, or installation of personal firewall or host-based intrusion prevention technology on systems that are going to be vulnerable for a long period of time. Patch management should also be augmented with network access control (NAC) to protect the IT environment from systems that are on the network, cannot be patched and are corrupt. NAC will

augment patch management functions for systems such as highly mobile corporate laptops that cannot be patched quickly and unmanaged systems that cannot be patched.

RECOMMENDED READING

"Identifying and Solving Vulnerability Management Weak Spots"

"Finding and Solving Vulnerabilities in Embedded Operating Systems"

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509