

PATCH MANAGEMENT

February 2008

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary	2
I. Trends and Zero-day Attacks	3
II. Patch Management Deployment.....	4
Preparation	4
Vulnerability Identification and Patch Acquisition.....	5
Risk Assessment and Prioritisation.....	7
Patch Testing.....	8
Patch Deployment and Verification	9
Patch Distribution and Application Tools.....	9
III. Patch Management Governance	11
Security Considerations	12
Criteria for Choosing a Patch Management Solution	13

SUMMARY

According to the CERT Coordination Center (CERT/CC), thousands of software vulnerabilities are discovered and reported every year¹. A flexible and responsive security patch management process has become a critical component in the maintenance of security on any information system. As more and more software vulnerabilities are discovered and therefore need updates and patches, it is essential that system administrators manage the patching process in a systematic and controlled way. This paper provides a core set of principles and methods that can be used as a reference in putting together an effective patch management programme.

¹ http://www.cert.org/stats/vulnerability_remediation.html

I. TRENDS AND ZERO-DAY ATTACKS

According to statistics published by CERT/CC, the number of annual vulnerabilities catalogued has continued to rise, from 345 in 1996, to 8,064 in 2006². Put another way, identifiable software vulnerabilities have increased more than 20 times over the last decade.

On top of this, attackers are able to take advantage of newly discovered vulnerabilities in less time than ever. It has been shown that the amount of time between the discovery of a software vulnerability and corresponding attacks has been steadily decreasing. There is also an increasing trend towards attack tools that exploit newly discovered vulnerabilities appearing well before any corresponding patch is released by the software vendor to fix a problem. This situation is generally known as a “zero-day attack”.

A large percentage of the incidents reported are caused by successful exploitation of a relatively small number of vulnerabilities in systems and applications³. To avoid attacks through known issues or vulnerabilities, organisations should make sure all IT system administrators are fully up to date with the latest security patch/hot-fix releases from their software vendors. Patches and updates should be reviewed regularly and applied to the operating system and/or applications that make up the organisation’s information systems. The patch management process should be timely and responsive. To accomplish this, the patching process should be managed in a systematic and controlled way.

² http://www.cert.org/stats/vulnerability_remediation.html

³ <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

II. PATCH MANAGEMENT DEPLOYMENT

Successful Patch Management requires a robust and systematic process. This process, the Patch Management Lifecycle, involves a number of key steps: preparation, vulnerability identification and patch acquisition, risk assessment and prioritisation, patch testing, patch deployment and verification.

PREPARATION

The following are suggested as part of the preparation process:

1. Create and maintain an pan-organisational hardware and software inventory

System administrators should create and maintain a clear inventory record of all hardware equipment and software packages, along with version numbers of those software packages most used within the organisation. This inventory will help system administrators better monitor and identify vulnerabilities and patches that are applicable across the organisation.

2. Standardise configurations

Standard configurations should be created and maintained for every major group of IT resources, such as user workstations and file servers. Standardised configurations can simplify the patch testing and application updating process, and will reduce the amount of time/labour devoted to patch management.

3. Educate users

Information security is everybody's business and an effective patching process cannot be implemented without the cooperation and participation of end-users across the organisation. Users should be made aware of the importance of IT security and patch management as part of their daily work process. If sufficient training is provided to end-users, they can often perform lightweight patching on their own workstations, which will reduce the workload on system administrators around basic patch management. User awareness is especially

important in organisations that allow remote access to a corporate network, as a vulnerability exploited through a computer system in someone's home can threaten the security of the entire organisation.

VULNERABILITY IDENTIFICATION AND PATCH ACQUISITION

There are a number of information resources available to system administrators in order to monitor vulnerabilities and patches that may be applicable to their installed hardware and software systems. As each type of resource has its own specialised area, system administrators need to be able to refer to more than one source for accurate and timely information on new vulnerabilities and patch releases.

Some common resources are:

1. Product vendor websites and mailing lists

Product vendor websites are probably the most direct and reliable resources for system administrators on vulnerability and patch related information for specific products. Many large vendors also maintain support mailing lists that enable them to broadcast notifications of vulnerabilities, patches and updates to subscribers via email. However, it should be noted that vendors sometimes do not report new vulnerabilities straight away, as they may not wish to report a specific vulnerability until a patch is available. It is therefore necessary to track other IT security resources for timely vulnerability and patch information.

2. Third-party security advisory websites

A third-party security advisory website is one that is not affiliated with any one vendor, and may sometimes provide more detailed information about vulnerabilities that have been discovered. These websites may cover a large number of products and report new vulnerabilities ahead of the product

vendors because, as mentioned, some vendors may choose to hold a vulnerability notification until a patch is available.

These third-party vulnerability advisory websites can be divided into two categories: websites run by Computer Emergency Response Teams (CERTs) and websites run by security vendors.

a) Security advisory websites run by CERTs

One of the most popular vulnerability advisory websites is the US CERT/CC site. It provides technical information about any newly uncovered vulnerability that can assist system administrators and security professionals in assessing the threat from the vulnerability. These advisories are updated as soon as new information is available from the product vendors.

b) Security advisory websites / resources run by security vendors

A number of third party mailing lists, such as NTBugTraq⁴ maintained by CyberTrust, and BugTraq⁵ maintained by SecurityFocus, are popular with IT professionals. However, system administrators should verify the information released in these websites with product vendors to confirm the accuracy of any newly discovered vulnerabilities. These websites may also offer newsgroups that system administrators can use to communicate with other users in the same field. System administrators should be careful not to release sensitive information through joining and using these mailing lists and newsgroups.

To assist in the task of keeping up to date with patch releases and vulnerability reports, a number of vulnerability alert services have been developed that allow system administrators to receive automated and customised notification on any

⁴ <http://www.ntbugtraq.com/>

⁵ <http://www.securityfocus.com>

vulnerabilities in and across the specific systems they are responsible for. Some services are free to use, while others require a subscription fee. The Talisker website maintains a list of currently available vulnerability alert services⁶. An RSS feed is also available that system administrators can subscribe to and keep abreast of newly discovered vulnerabilities.

RISK ASSESSMENT AND PRIORITISATION

Timely response is critical to effective patch management. With limited resources, system administrators may need to prioritise the deployment of new patches, performing a risk assessment to determine which systems should be patched first. In general, this prioritisation should be based on the following criteria:

1. **Threat** – A threat is any potential direct danger to information systems. Examples of systems facing high threat levels are web servers, email servers and servers containing sensitive information.
2. **Vulnerability** – A vulnerability signifies the absence of, or a weakness in, a safeguard which could be exploited by an attacker. It could be a flawed software service running on a server, or unrestricted modem dial-in access, and so on.
3. **Criticality** – This is a measure of how important or valuable a system is to business operations. Systems that are frequently considered as mission critical include mail servers, database servers and network infrastructure.

In general, systems facing more threats, or that are more vulnerable, or are mission critical should be accorded a higher priority in the patch management process.

⁶ <http://www.securitywizardry.com/alert.htm>

System administrators should identify the associated risks and actions that need to be taken once a security vulnerability has been confirmed (for example, scheduling system down time for reboot after installing a patch), and assess any impact associated with installing a security patch once that patch becomes available. Before applying a patch, system administrators need to ensure that the new patch is not going to affect the overall functionality of the system and its applications (see next section).

PATCH TESTING

Patch testing is vital to ascertain whether or not a new patch will affect the normal operation of any existing software. It is important that this testing is performed on a mirror system that has an identical or very similar configuration to the target production system. This is to ensure that the patch installation does not lead to any unintended consequences on the production system.

In addition to identifying any unintended problems, patches themselves should be tested to ensure that they have fully patched the vulnerability in question or corrected the performance issue as intended. This can be accomplished by:

1. Checking that the files or configuration settings that the patch is intended to correct have been changed as outlined in the vendor's documentation.
2. Scanning the host system with a vulnerability scanner that is capable of detecting known vulnerabilities. This technique however may not always be effective because vulnerability scanners may not check for the actual presence of the vulnerability in question. Many vulnerability scanners only check software version numbers or patch levels to determine whether vulnerabilities exist or not.

If it is not feasible to install the patch because, for example, testing results show that the patch will crash or seriously disrupt the production system, alternate security controls should be implemented.

PATCH DEPLOYMENT AND VERIFICATION

Patching vulnerabilities in a system may be as simple as modifying a configuration setting, or it may require the installation of a completely new version of the software. No single patch method can apply across all software applications and operating systems. Product or application vendors may provide specific instructions for applying security patches and updating their products, and it is recommended that system administrators read all the relevant documentation provided by vendors before proceeding with patch installation.

In addition, security patches should be deployed through an established change control process. Before applying a new patch, administrators may want to conduct a full backup of the system to be patched. This enables a quick and easy restoration of the system to a previous state if the patch has an unintended or unexpected impact on the system. After the patch is deployed, system administrators and users should verify that all systems and applications are functioning normally, and that they comply with laid down security policies and guidelines.

PATCH DISTRIBUTION AND APPLICATION TOOLS

Organisations may want to consider using automated patch management tools to speed up the distribution and installation of patches., There are a number of patch management systems in the market that can help automate the entire patch management process. There is also a website⁷ run by patchmanagement.org that maintains a list of patch management vendors who offer solutions performing both

⁷ <http://patchmanagement.org>

patch assessment and remediation⁸. They also maintain a page linking to patch management product comparisons previously published in industry magazines⁹.

Patch management systems can be broadly categorised into two areas:

1. Cross-platform patch management systems

This category of products can handle patches from more than one operating system, or products from different vendors.

2. Platform specific patch management solutions

This category of products will only support patches from a specific vendor or platform. A well-known example is the patch management tools provided by Microsoft. *Microsoft Windows Server Update Services (WSUS)* is a free tool from Microsoft designed to help system administrators deploy the latest Microsoft product updates and patches to computers running the Windows operating system.

⁸ <http://patchmanagement.org/vendors.asp>

⁹ <http://patchmanagement.org/comparisons.asp>

III. PATCH MANAGEMENT GOVERNANCE

All organisations need to protect information systems from known vulnerabilities and security risks by applying the latest patches recommended by product vendors, or implement other compensatory security measures. Patch management should be based on an assessment that balances the security and down time risk of a security breach with the cost, disruption and availability risks associated with frequent and rapid deployment of software patches.

Before security patches are applied, proper risk evaluation and testing should be conducted to minimise any undesirable effects to the normal running of information systems. A clear operational process that enables rapid testing and deployment should be established.

Depending on the nature of information systems in question, risk levels may be different. For example, an information system that is only used internally faces fewer threats than an information system that directly interfaces with the Internet, serving customers or the general public. Depending on the risk level, organisations should determine the appropriate patch management strategy for each of their systems, including patch checking and patching frequency. In short, high-risk information systems should be addressed first.

When evaluating whether to apply a security patch or not, the risks associated with installing the patch should be assessed. Compare the risk posed by the vulnerability with the risk of installing the patch. If an administrator decides not to apply a patch, or if no patch is available, there should be other compensating controls. These may include:

1. turning off services or capabilities related to the vulnerability
2. adapting or adding access controls

3. increased monitoring of systems to detect and prevent actual attacks.

SECURITY CONSIDERATIONS

When deploying a patch management solution, the following security issues should be considered:

1. The patch management system itself is a software application, and it might have its own set of security vulnerabilities. Patches to the patch management system and its components should be applied as soon as possible.
2. The servers that are running a patch management solution should be properly protected because this will be a central distribution point, sending updates to virtually all machines in the organisation. It could prove disastrous if the files in the patch management servers were to become infected with a virus. Any anti-virus software running on the server should have auto-protection enabled with the latest virus signatures and malicious code definitions installed in order to protect against any virus outbreak.
3. Access control to the patch management system should be secured, both physically, by limiting physical access to the central console to authorised personnel only, and logically, by restricting access to the central console to pre-registered IP addresses only.
4. Communication channels into the patch management system should be properly secured and protected. An attacker may be able to sniff network communications for sensitive information such as authentication credentials or patching statuses to determine which patches have been installed on particular systems, and hence locate vulnerable attack targets. Security measures such as data encryption should therefore be put in

place to protect sensitive information passing through the management system from leakage¹⁰.

5. Regular IT security risk assessments and audits should be conducted on the patch management system.

CRITERIA FOR CHOOSING A PATCH MANAGEMENT SOLUTION

Besides matching the specific user and business requirements, including product functionality and budget constraints, organisations should also take the following factors into consideration when considering a robust and secure patch management solution:

1. **Fewer Vulnerabilities:** Some patch management products have more vulnerabilities than the others. Organisations should choose an appropriate solution that looks less likely to be vulnerable itself, which in turn will reduce the need to patch the software regularly. Research should be conducted first to independently verify the product concerned. A complex product may mean more code and services that in turn might introduce more vulnerabilities. It may be wise to select a less complicated and more mature product;
2. **System Compatibility:** Some patch management solutions are agent-based and some are agent-less. Organisations should evaluate any impact to their systems (such as performance, stability and compatibility), if agents are to be deployed across a large number of machines;
3. **Vendor Responsiveness to New Vulnerabilities:** Organisations should also take note of the speed with which the solution vendor responds to new vulnerabilities with patches and updates;

¹⁰ <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

4. Ease of Deployment and Maintenance: The easier the patch management solution is to deploy and maintain, the lower the implementation and ongoing maintenance costs to the organisation;
5. Audit Trail: A good patch management solution should provide comprehensive logging facilities, that help system administrators easily keep track of the status of software fixes and patches on individual systems.