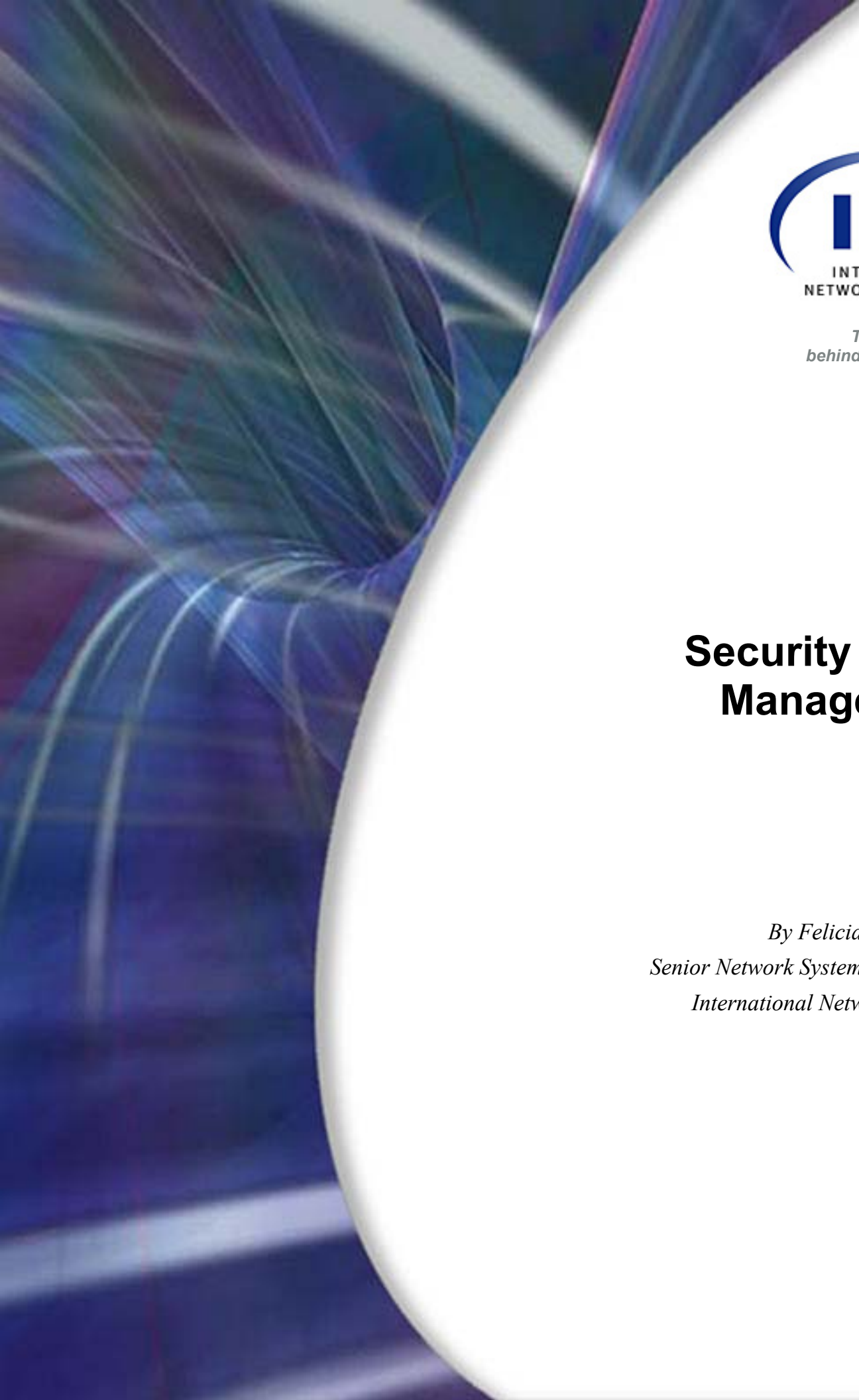

INS
INTERNATIONAL
NETWORK SERVICES

The knowledge behind the network.®

Security Patch Management

By Felicia M. Nicastro
Senior Network Systems Consultant
International Network Services

Security Patch Management

High Level Overview of the Patch Management Process

By Felicia M. Nicastro, Senior Network Systems Consultant

Introduction

A rigorous patch management process is a fundamental security requirement for any organization doing business today. Such a program ensures that the security vulnerabilities affecting a company's information systems are addressed in an efficient, thoughtful, timely and effective manner. This process introduces a high degree of accountability and discipline to the task of discovering, analyzing and correcting security weaknesses.

The patch management process is a critical element in protecting any organization against emerging security threats. Formalizing the deployment of security-related patches should be considered one of the key elements in a Security Group's program to enhance the safety of information systems for which they are responsible. The intent of this whitepaper is to serve as a starting point for an organization to practice secure patch management procedures.

Background

Information security advisory services and technology vendors routinely report new defects in software. In many cases, these defects introduce opportunities to obtain unauthorized access to systems running this software. Information about security exposures often receives widespread publicity across the Internet, increasing awareness of software weaknesses, with the consequential risk that cyber criminals could attempt to use this knowledge to exploit vulnerable systems. This widespread awareness leads vendors to quickly provide security patches so they can show a response to a vulnerability that has been publicized and avoid erosion of customers' confidence in their products.

Historically, most organizations tend to tolerate the existence of security vulnerabilities and, as a result, deployment of important security-related patches is often delayed. Most attention is usually directed toward patching Internet-facing systems, firewalls and servers, all of which are involved in data communications to business partners and customers. These preferences resulted from two fundamental assumptions:

- The threat of attack from insiders is less likely and more tolerable than the threat of attack from outsiders.
- A high degree of technical skill is required to successfully exploit vulnerabilities, making the probability of attack unlikely.

In the past, these assumptions made good, practical sense and were certainly cost-effective given the limited scope of systems. However, the threat profile and potential risks to an organization have both changed considerably over time. Viruses can now be delivered through common entry points (such as e-mail attachments), automatically execute, and then search for exploitable vulnerabilities on other platforms. This

was once just a theoretical threat, but became a reality with the release of the Nimda virus in September 2001.

With this in mind, the Security Group within an organization should develop a formal process to be used to address the increased threats represented by security vulnerabilities. This whitepaper introduces and explains the elements of a security patch management process to meet the challenges vulnerabilities represent.

Process Lifecycle

A patch management process describes best practices that should be employed in any major organization to govern how to respond to security vulnerabilities. This process is implemented whenever the organization becomes aware of potential security vulnerability and whenever a vendor releases a new patch to address security vulnerability.

The process covers the following key activities:

- Monitoring for security vulnerabilities from security intelligence sources
- Completing an impact assessment on new security vulnerabilities
- Developing and testing the technical remediation strategy
- Implementing the technical remediation strategy on all effected hosts
- Documenting the lifecycle of each vulnerability, including reporting and tracking of remediation measures implemented by each line of business
- Integrating the patch or configuration changes into the related application/system baseline and standard build

Roles and Responsibilities

The patch management process should define the roles and responsibilities of groups and individuals who will be involved in remediating a known vulnerability. A description of these groups and individuals follows.

CIRT

A local Computer Incident Response Team (CIRT) manages the analysis and management of security vulnerabilities. The CIRT should have the ability to call on subject matter experts (SMEs) from other parts of the organization for additional expertise.

The CIRT's responsibilities include:

- Monitoring security intelligence sources for new security vulnerabilities
- Responding within 24 hours to any request from any employee to investigate a potential security vulnerability
- Defining and promoting awareness of escalation chains for reporting security vulnerabilities
- Engaging employees or contractors to play lead roles in:
  - Vulnerability analysis
  - Patch identification
  - Test plan development
  - Formal testing
  - Development of action plans

- Coordinating the development of action plans with timetables for addressing vulnerabilities
- Coordinating the approval of security-related patches
- Notifying all groups about tools and implementation and back-out plans
- Managing documentation

Product Managers

In larger organizations, the IT group can contain product managers who are usually responsible for a specific product or application (e.g., Windows, UNIX, Apache, MySQL). Product managers' responsibilities can include:

- Responding within 24 hours to requests from the CIRT to assist in the analysis of security vulnerabilities and development of a suitable response
- Maintaining a list of qualified employees within an organization to act as SMEs on different technologies
- Calling and attending relevant meetings, as required, to determine the impact of new vulnerabilities on the systems for which they are responsible
- Leading the development and testing of remedial measures through their engineering groups
- Ensuring evaluation of the testing results prior to patching or solution implementation
- Making recommendation on the approach to remediation, especially when a vendor patch is not currently available – and until it becomes available

Information Risk Managers

Typically, information risk managers (IRMs) are responsible for ensuring the data they are responsible for is secured according to corporate security policy. IRMs are included in the patch management process since they must ensure that a vulnerable system within their realm is patched before it is exploited. IRMs' responsibilities should include:

- Assisting the CIRT in analyzing the impact of security vulnerabilities within their respective departments
- Assisting coordination of the development of security related patches within their business

Operations Manager

Operations managers, also known as an information technology managers, are usually responsible for deploying the patch on the vulnerable systems. They are important members of the security patch management process since they must coordinate the patch implementation efforts. Operations managers' responsibilities should include:

- Assisting the product manager in developing the action plan and timeframes for completion
- Be involved during the development and testing phase to monitor progress and provide insight
- Be responsible for deployment of the remedial measure to eliminate security vulnerabilities

Analysis

Monitoring and Discovery

Once established within an organization, the CIRT is then responsible for daily monitoring of all appropriate security intelligence sources for exposures that may impact platforms or applications utilized by the organization. (Note: New security advisories and patches for vulnerabilities are released frequently; therefore diligence on the part of CIRT will be required at all times.)

Intelligence sources will normally publish a detailed, formal announcement of a security vulnerability. Announcements usually provide a description of the vulnerability, the platform or application affected, and the steps necessary (when available) to eliminate the risk. In addition, employees or contractors outside of the CIRT may become aware of vulnerabilities through personal sources, including hands-on experience and word of mouth. They should be encouraged through security awareness training and regular communications from the CIRT to report these to the CIRT.

The following websites and mailing lists are examples of security intelligence sources:

- General Security
  - SecurityFocus.com: http://www.securityfocus.com
  - InfoSysSec: http://www.infosyssec.net
- Mailing Lists
  - Bugtraq Archive: http://www.securityfocus.com/archive/1
  - NT Bugtraq: http://www.ntbugtraq.com
- Advisories
  - Computer Emergency Response Team: http://www.cert.org
  - SecurityFocus.com: http://www.securityfocus.com
- Vendor Security Resources
  - Microsoft: http://www.microsoft.com/security
  - Sun Microsystems: http://sunsolve.sun.com
  - Hewlett-Packard: http://www.hp.com
  - IBM: http://www.ibm.com
  - Linux Security: http://www.linuxsecurity.com

Initial Assessment

Once a vulnerability that affects a platform or application in use within the environment has been identified, the CIRT should perform an initial review to establish the resources required to perform adequate analysis of the vulnerability and to establish an initial level of exposure. This should be completed within 48 hours of the vulnerability being identified. These resources would include other groups from within the company, primarily Product Management and SMEs from other groups, but will often also include product vendors.

Impact Assessment

CIRT and the product manager would then assess the impact of the vulnerability on the environment. Product managers are included in this phase of the process because they have product engineering responsibility and a detailed technical understanding of the product.

Assessing the impact requires developing a risk profile, including the population of hosts that are vulnerable, the conditions that need to be satisfied to exploit the vulnerability, and the repercussions to the company if it were to be exploited.

Factors considered in the impact assessment will include:

- **Type and delivery of attack** – Has an exploit for the vulnerability been published? Is the vulnerability at risk of exploitation by self-replicating, malicious code?
- **Exploit complexity** – How difficult is it to exploit the vulnerability? How many conditions must be met in order to exploit it? What infrastructure and technical elements must exist for the exploit to be successful?
- **Vulnerability severity** – If the vulnerability is exploited, what effect will this have on the host?
- **System criticality** – What systems are at risk? What kind of damage would be caused if these systems were compromised?
- **System location** – Is the system inside a firewall? Would it be possible for an attacker to use a compromised host as a beachhead for further attacks into the environment?
- **Patch availability** – Are vendor-supported patches available? If not, what steps can be taken to lessen or eliminate the risk?

Note: If both the CIRT and the product manager conclude that the security vulnerability has no impact on the environment, no further action is needed. A record of all information gathered to date would be stored by the CIRT for future reference.

Timeframe

The CIRT, in conjunction with the operations manager, would need to define a timeframe for the deployment of the security patch based on the criticality of the vulnerability and any other relevant factors.

Remediation

Course of Action

Once the risk or exposure is known and documented, Product Management would then develop a course of action for the vulnerability for every platform or application effected. This will be performed with the input of the CIRT, when necessary.

The course of action may consist of:

- Applying a vendor-supplied patch, either specific to the vulnerability or addressing multiple issues
- Modifying the functionality in some way, perhaps by disabling a service or changing the configuration

When a vulnerability affects a vendor-supplied product and the vendor has not supplied an appropriate patch or workaround, the product manager will work with the vendor to develop an appropriate mitigation strategy. Regardless of the vendor's recommendation, the product manager needs to determine and document the course of action that is to be taken. When a vendor-supplied patch is to be used, Product Management will be responsible for retrieving all relevant material from the vendor.

Note: Binary patches are a potential vector for a Trojan Horse or self-replicating malicious code. As such, verifying the authenticity of all patches with the vendor, preferably through the use of digital signatures, is important.

Testing

Testing is coordinated through the product manager and includes services from appropriate SMEs and access to necessary resources (e.g., test labs). The product manager is responsible for preparing a detailed implementation plan and performing appropriate testing in a representative lab environment. A formal plan and documentation to govern the testing will be generated based on the type of system and vulnerability. Formal testing is conducted, and documented test results are provided to the CIRT. A back-out plan would also be developed and tested to ensure that if the patch adversely affects a production system, it can be quickly reversed and the system restored to its original state.

Back-out procedures could include:

- Vendor-specific procedures to remove the patch or fix
- Other backup and restore procedures to bring a disrupted system back to its original state

The product manager is responsible for approving the implementation plan for production use based on the test results and recommendations from SMEs and information security professionals. The product manager must also validate that the patch is protected from malicious activity before it is installed on the system. This is usually done in the form of MD5 hash functions implemented by the vendor prior to distribution.

Standard Build

When a standard build for a platform or application is impacted by a vulnerability, it must be updated to avoid replication of the vulnerability. This ensures that any future implementation of a platform or application has the modifications necessary to eliminate the vulnerability.

A timeframe for deploying the updates into the build must be determined in the remediation phase. It must be carefully set to ensure a build is not updated too frequently, risking the validity of appropriate testing, and not too sparsely, such that new implementations are procured without the fix or update to address the security vulnerability.

Security Advisory

Once an appropriate course of action has been agreed upon and tested, the CIRT will release an internal Security Advisory. The Security Advisory is always issued using the template provided in order to show consistency and reduce confusion. Each Security Advisory contains the following information:

- **Vulnerability description** – the type of vulnerability, the effected application or platform versions, and methods used to exploit it
- **Implementation plan** – detailed instructions on the steps required to mitigate the vulnerability, including the location of repositories containing executable programs, patches or other tools required
- **Back-out plan** – details on how to address unexpected problems caused by the implementation of the remedial measures
- **Deployment timeframe** – a deadline for applying remedial measures to vulnerable systems. Systems with different levels of risk may have different timeframes to complete the deployment.

The audience that receives a notification will depend on the nature of the advisory.

Critical Vulnerabilities

In situations where a vulnerability introduces a significant threat to the organization, awareness must be promoted. This will include a staged release of notifications with the intent of informing IRMs before awareness of the vulnerability is promoted to others. Other stakeholders within the business areas will generally be notified shortly after the discovery of a vulnerability that requires a response from the organization.

Update Operational Environment

Distribution

The product manager distributes all files, executable programs, patches, or other materials necessary to implement the mitigation strategy to the appropriate operations manager by using an internal FTP or web site. The product manager is responsible for ensuring the data is transmitted via a secure method that meets integrity requirements.

Implementation

The Operations Group will apply patches in accordance with established change management procedures. Following the implementation, the Operations Group is responsible for testing production systems to ensure stability. Production systems may experience disruption after a security patch has been applied. If this occurs, the defined back-out procedures should be implemented.

Exceptions

In exceptional cases, a business unit may be unable or unwilling to implement mitigating measures within the required timeframe for the following reasons:

- The system isn't vulnerable to the threat due to other factors
- The vulnerability is considered a limited threat to the business
- The security-related patch is determined to be incompatible with other critical applications

In such cases, the business unit may submit an action plan to the CIRT to pursue alternate mitigation strategies. If a business unit wants to delay the implementation of the security patch, the IRM must complete a risk acceptance form, which details any risks resulting from the failure to deploy the patch. The risk acceptance form is presented to the CIRT.

Tracking

It is necessary to ensure that any security vulnerability is properly mitigated on all platforms or applications affected throughout the environment. IRMs are responsible for tracking the progress in updating the operational environment during the security patch management process.

The tracking process includes detailing each vulnerable system, the steps taken to eliminate the risk, and confirming that the system is no longer vulnerable. Any exception made to a vulnerable system must also be included in the tracking process. A standardized form will be specified to record when a system has been patched. The tracking results will be reported to CIRT in accordance with the timetable set out in the Security Advisory.

Reporting

The CIRT will maintain consolidated reporting on each security vulnerability and affected system. For each vulnerability, the following documentation will be maintained by the CIRT:

- Vulnerability overview with appropriate references to supporting documentation
- Test plan and results for relevant security-related patches or other remedial measures
- Detailed implementation and back-out plans for all affected systems
- Progress reports and scorecards tracking systems that have been patched

All supporting documentation for a processed security vulnerability is stored in the CIRT database (which is a restricted data storage area, available only to the CIRT members and designated information security specialists). The CIRT publishes a list of security-related patches that have been determined to be necessary

to protect the organization. This list is reissued whenever a new security-related patch is sanctioned by the CIRT.

An online system is used to report status. System owners are required to report progress when deploying required remedial measures. When feasible, the CIRT monitors vulnerable systems to ensure that all required remedial measures have been successfully implemented.

A scorecard is used in the reporting process to ensure that any vulnerable system is in fact fixed. The CIRT is responsible for creating and maintaining the accuracy of the scorecard for each system affected by the vulnerability. The scorecard must be monitored and kept up to date to ensure there are no outstanding issues.

Conclusion

For an organization to implement a sound patch management process, time and dedication need to be given up front to define a solid process. Once the process has been put in place, the cycle will begin to take on a smoother existence with each release of a security vulnerability. Sometimes, the most difficult hurdle is determining how to approach a patch management process. Of course, in smaller organizations, the CIRT may actually be a single individual instead of a team, and the tasks may also be broken down and assigned to specific individuals instead of in a team atmosphere. With the release of vulnerabilities today occurring at a rapid rate, it is better to address a vulnerability before an exploit is executed within your infrastructure. The patch management process can reduce the risk of a successful exploit, and should be looked at as a proactive measure, instead of a reactive measure.

About INS

INS (International Network Services Inc.) is a leading global provider of vendor-independent network consulting and security services. We offer a full range of consulting services to help companies build, optimize, manage, and secure their network infrastructures to enable their business initiatives and achieve a sustainable operating advantage. INS is a recognized leader in business-critical, multivendor network consulting, having helped more than 75% of the Fortune 500 and delivered more than 15,000 engagements over the past decade. Headquartered in Santa Clara, CA, INS has regional offices throughout the United States and Europe. For additional information, please contact INS at 1-888-767-2788 in the U.S., 44 (0) 1628 503000 in Europe, or 1-650-318-1020 worldwide, or visit www.ins.com.