

BITS

FINANCIAL SERVICES
R O U N D T A B L E

PATCH MANAGEMENT BEST PRACTICES FOR IT PRACTITIONERS JULY 2004

Organizations are increasingly dependent on effective software patch management to secure their operations. The time between the announcement of a vulnerability and the appearance of an exploit is shrinking. In this environment, speeding the process of testing and deploying software patches is critical. Companies must be able to rapidly deploy software and system updates in order to offer continuous services and interconnectivity with partners and customers.

Effective patch management practices are important for software providers and users. Regulators and security experts have published supervisory requirements and best practices. BITS issued its Business Requirements for Software Security, urging software providers to produce higher quality software with fewer security vulnerabilities and a more efficient process for managing patches.

This document, “Patch Management Best Practices for IT Practitioners,” is intended to assist IT practitioners at financial services companies in implementing a more robust patch management process. This document is not intended to be a comprehensive overview. Instead, it is a high-level summary of the risks and steps financial institutions should consider in developing a strategy for evaluating, testing and implementing patches. For a list of sources used to compile these practices, please see Appendix A.

The Business Problem

Attacks on corporate information networks in recent years have heightened companies’ awareness of vulnerabilities and exploits, making information security one of the top risk management challenges. Financial institutions recognize the importance of mitigating these threats in a timely and appropriate manner. Failure to do so can have severe consequences, from service disruptions of mission-critical systems, to breaches of confidential customer information, to the overall failure of a financial institution due to the damage to its reputation. An organization can even be held legally responsible for damages if its unsecured systems are used to attack others. While corporations have taken significant steps to secure their networks against digital threats from outside the corporate firewall, providers and users of software must remain vigilant to ensure networks remain secure.

Software patches may not always be available when the attack is discovered. An exploit that is launched before a patch is available is known as a zero-day event. To prepare for a zero-day event, companies should know how they will respond to certain scenarios and be prepared to deploy those responses. These scenarios may affect all or part of the business. In order to prepare for these situations, companies should ensure that a security incident response process is in place to quickly assemble a team to assess the threat and enact appropriate technical mitigants. In addition, this should tie into a company’s business recovery plan to ensure that business impacts are communicated in a timely and effective manner. Depending on the circumstances,

drastic action may be necessary to protect information assets, maintain service, preserve the institution's reputation, and limit liability exposure.

Develop Security Policy, Procedures and Toolset

Patch management is one component of corporate risk management and a subset of both risk- and change-management processes. An enterprise patch management strategy should start with:

- An explicit and documented organizational security policy;
- Systematic, accountable, and documented processes and procedures for handling patches across the enterprise; and
- Comprehensive toolsets that track and monitor requirements.

Determining the risk appetite of a company is often the most difficult step in implementing a patch management strategy. A severity-rating matrix can help.¹ Severity ratings may vary based on risk tolerance of individual companies.

Production environments are often the initial focus of any urgent deployment, leaving backup, contingency, test and QA environments unpatched and the company exposed. Patch- and vulnerability-management processes and procedures should specify how the company will monitor for new patches and vulnerabilities and identify personnel responsible for assessing, testing, installing and monitoring patches.

Organizations should communicate the patch management policies to remote users, including third-party service providers. The patch management requirements should be incorporated into third-party contracts. Remote users accessing corporate assets are often the weakest link in a company's defense. For example, if there is a serious worm or virus spreading on the Internet, a company could—as documented in its security incident response process—have a process to disable employee remote access until things are safe and the technical staff can monitor for risks. This can help when technical staff are busy protecting corporate assets.

Define Roles, Responsibilities and Tools

An organization's patch management process should define the roles and responsibilities of groups and individuals involved in remedying vulnerabilities. Some organizations may establish a dedicated patch management group. Others may assign responsibility based on related duties.² Organizations should also appoint a patch management sponsor. This individual enforces company software patching standards and compliance with the patch management policy. Individuals who are responsible for the patch management process should understand their organization's risk tolerance with respect to installing patches and help to identify and distribute patches in the organization, using the organization's severity rating as a guide.

The patch deployment strategy may be automated or manual. An automated method is recommended for organizations of all sizes, since the large number of patches can quickly overwhelm the resources assigned to manually patch any environment and is generally cheaper. While some smaller organizations install patches manually, this becomes increasingly difficult as organizations centralize services and standardize desktop configurations.

A number of vendors offer automated patch management tools. This document does not address the advantages and disadvantages of specific tools. The categories of tools related to the patch management process include, but are not limited to, enforcement, inventory, verification, compliance, implementation, and reporting.

¹ See Appendix B for a sample severity-rating matrix.

² See Appendix C for a sample of roles and responsibilities.

Organizations should consider the following when evaluating an automated patch management and deployment solution:

- Platform coverage;
- Research depth;
- Workflow;
- Controlled rollout;
- Rollback;
- Reporting; and
- Validation.

Patch management strategies should not be delayed as companies search for a comprehensive solution. Instead, organizations should use available tools (preferably within the organization) to automate patch deployment. The tool and process used to deploy the patch should be evaluated and tested to meet the company's specific requirements. The company should consider any previously implemented tools that automate patch deployment.

How patches are deployed should vary according to the severity of the vulnerability. Deploying patches for vulnerabilities rated "critical" involves a higher level of risk to company assets and thus is different than for vulnerabilities rated "high", "moderate" or "low." The following is an example of a high-level patch management process:

1. A security bulletin or alert is published by a software vendor.
2. The company information security office and/or the corporate information technology provider (whether internally or externally supported) assesses the risk to the company. The company information security office recommends an internal severity rating. This should be done within 48 hours.
3. The corporate information technology provider (whether internally or externally supported) release(s) a patch after verifying its authenticity and integrity (by scanning it for viruses and installed on an internal system or other verification processes).
4. The patch is tested on standard build image with representative business applications. For patches rated critical by your organization, this should be completed within 48 hours.
5. The company's automated deployment tool is configured for the patch.
6. The patch is deployed based on the operational windows available to implement it. The operational window is defined through an assessment of the urgency of the patch and the operational impact of its deployment.
7. The company issues a status report of the deployment to the appropriate process owner.
8. Accountability reports are distributed to appropriate senior management by an independent internal group to assess compliance to policy.

Patches for non-critical vulnerabilities are deployed operationally. These patches must be tested and approved by application owners and business partners before being deployed. Assessment, testing, and verification require significant coordination and resources. The time for deployment for each patch will vary based on the complexity of the patch.

With a critical vulnerability, the risk of the vulnerability affecting company business is greater than the risk of deploying a patch and affecting user productivity. In most cases, companies decide that the risk of the patch breaking some systems is lower than the risk involved in leaving systems vulnerable. As a result, critical patches are typically automated and often are easier to manage than patches deployed operationally.

Develop and Maintain an Inventory of IT Infrastructure

The threat of an attack determines the vulnerability's severity rating and the urgency of deploying the patch. Therefore, companies must be able to assess quickly their risk to a particular vulnerability. An accurate IT inventory can help assess risk. Organizations should develop and maintain an up-to-date hardware and software inventory of the entire IT infrastructure that includes:

- Production systems;
- IP addresses;
- Patch status;
- Patch level;
- Vulnerabilities;
- Physical location of the patch;
- Custodian of the patch; and
- Function of the patch.

Commercial inventory tools, from general network scanners to automated discovery products, can expedite the IT inventory process. If multiple tools are used for an IT inventory, additional resources will be needed to cross-reference inventory reports.

The inventory should be updated frequently and must include relevant third-party service providers. It should be made available to everyone in the organization who might need it, such as network executives, security managers, and system administrators. Enforcement of asset inventory, virus protection, and vulnerability-mitigating tools should be part of both a company policy and a technical solution. A single, accurate asset inventory, preferably integrated with a patch management tool, is critical to the success of the company's information security program.

Organizations may discover nonstandard and noncompliant products as part of their asset inventory. If left unpatched, these products can be a risk and carry possible legal and support issues. Relevant stakeholders should sign off on these products/issues. A policy and a technical solution should be developed to address and track noncompliant and nonstandard products.

Develop a "Standard Build"

A standard build for the desktop and servers ensures consistency across the enterprise. In most cases, standard builds are limited to the operating system. However, some organizations include the most commonly used applications and products in their standard builds. Establishing a standard build provides a quick glimpse into vulnerabilities that extend beyond the desktop/server level. This baseline helps companies quickly identify the current version and build of users and future patch application.

Large organizations often have difficulty maintaining a single desktop and server image. In complex businesses, business application requirements make multiple builds more appropriate. Organizations should minimize their number of standard builds, however, taking into consideration the cost and benefits of maintaining and patching each build. Maintaining multiple builds significantly escalates costs associated with patch deployment, problem management, and related processes.

Monitor Threats, Vulnerabilities, and Product Support

Depending on the complexity of the organization's systems, patches may be issued as frequently as several times a day. Organizations should establish a process and allocate resources for monitoring reliable sources in order to identify vulnerabilities, determine the impact of those vulnerabilities, and keep abreast of solutions. Organizations should scrutinize relevant information sources to determine which sites, sources and user

groups provide accurate and timely information. The Financial Services Information Sharing and Analysis Center (FS/ISAC) is a good source.

It is critical that organizations also monitor product lifecycles to understand the impact of unsupported products. Operating systems and vendor products should be kept up to date with the latest product release. Vendors typically will stop supporting older versions of their products. A company running a version of a product that is no longer supported will usually need to update the product before it can deploy a security patch for that product. Naturally, this adds to the complexity of the management process.

Assess Impact of New Vulnerabilities

An initial assessment is the first step in establishing a “triage” for patches. An organization’s patching process should include a method for deciding which systems are to be patched and which patches are installed first.³ Using its asset inventory, a company should determine which patches are applicable to the enterprise, including determining the severity of the vulnerability.

Not every enterprise needs to install every patch. Factors to consider in the impact assessment include:

- Type and delivery of attack;
- Severity of the vulnerability; and
- Criticality of the system.

Organizations should focus on the most critical updates first. For some vulnerabilities, there are compensating controls that can be used to allow companies time to patch all of their systems. In all cases, however, companies should document which patches are installed, the reason for not installing, and priorities for patching systems in the future.

In order to maintain a current inventory of systems and patches that require deployment, companies should make asset management and operational patch management a part of their company’s daily operational tasks. An operational procedure for patch management should:

- Ensure that once a device is patched it stays patched;
- Allow more flexibility in scheduling devices;
- Provide streamlined and consolidated status reporting;
- Minimize time required to deploy a patch;
- Manage orderly patch installation;
- Facilitate timely, company-wide risk assessment; and
- Help companies identify devices that need to be rebooted.

Test Patches

A patch management process should include a methodology for testing and safely installing patches. Once the patch is identified, the patch must be tested to evaluate its impact on the particular computing environment and to ensure that one security hole is not opened while closing another. The company should have a detailed implementation plan and the patch should be tested appropriately in a representative lab environment. In smaller environments, testing may be as simple as installing the software in a control group and using it in daily operations for a few days. In a large, complex environment, testing may take weeks in full test labs before the patch is ready to deploy. A back-out plan should also be considered to ensure that if the patch adversely affects a production system, it can be quickly reversed and the system restored to its original state.

³ See Attachment B for a sample severity matrix.

Testing should not be limited to the standard operating system build. Application testing also should be included in the testing cycle. Patch deployment can affect previously installed applications. The test plan should include testing of these applications and possible implications. A list of pilot or test users should be available to facilitate the application-testing phase of the patch management process.

Remediate Vulnerable Systems

Remediation is one of the most critical steps in protecting the enterprise. This is usually the most time-sensitive part of the patch management process, since patches must be applied to all appropriate systems.

Once the risk of exposure is known and documented, the responsible party(s) should develop a course of action for the vulnerability for every platform or application affected. High-level tasks associated with patch deployment include, but are not limited to, the following:

- Risk assessment;
- Patch testing and distribution;
- Progress reporting; and
- Exception handling.

Exceptions should be part of a company policy and should clearly provide evidence that the patch can not be installed. Exceptions to patch installation should be granted as infrequently as possible and should follow a formalized exception process. In the unusual circumstance that a patch cannot be deployed immediately, mitigating controls should be investigated and implemented. Vendor security bulletins typically include alternative workarounds that help minimize risk.

Verify Patch Installation

Organizations should verify the patch installation through network and host vulnerability scanning, including remote access to the network by employees and third-party service providers. Validation and reporting ensures that the systems and applications that require patches have actually been patched and the process is complete. Patch verification should be part of an ongoing assessment and should confirm that systems remain patched. The assessment verification should be conducted on a regular (e.g., daily, weekly, monthly) basis. This task requires ongoing review and enforcement by the technology service organization and information security. If enforcement is not adopted as a company policy, a successful patch assessment, deployment and verification strategy is difficult to achieve.

Workstation standard build refreshes should not be forgotten just because they are not part of the patch management process. Patches that are being deployed via the automated deployment tool should be included in the workstations build process.

Provide Training to Practitioners

The process outlined above will monitor for new patches and vulnerabilities found within the organizational inventory. Despite considerations outlined elsewhere in this document, local administrators may use software not listed in the inventory. In this situation, it is essential that local administrators are trained on the patch management processes. Through this training, companies create a second line of defense in the patching process.

Conclusion

Establishing a robust patch management process is an important part of a financial institution's information security program. Organizations should use this document to help develop a patch management process that assesses the risks and implements controls that adequately mitigate these risks.

Appendix: A - Sources

- *FDIC Guidance on Developing an Information System Patch Management Program to Address Software Vulnerabilities*, FIL-43-2003. See <http://www.fdic.gov/news/news/financial/2003/index.html>.
- *Information Security IT Examination Handbook*, Federal Financial Institutions Examination Council (FFIEC), December 2002.
- General Accounting Office (GAO) *Information Security Report: Effective Patch Management is Critical to Mitigating Software Vulnerabilities* – GAO-03-1138T
- National Institute of Standards and Technology (NIST): *Procedures for Handling Patches*, NIST Special Publication 800-40
- Network Reliability & Interoperability Council (NRIC) Best Practices. See <http://www.nric.org/>
- “Practical Patching,” *Information Security Magazine*, March 2003
- “A Patch in Time,” *Information Security Magazine*, February 2004
- National Cyber Security Partnership, “Improving Security Across the Software Development Lifecycle”, Cyber Security Task Force Patch Management Subgroup Report – Appendix C: Improving the Patch Management Process, <http://www.cyberpartnership.org/SDLCFULL.pdf>

Appendix B – Severity Rating Matrix Example

Rating	Criteria (One or more exist)	Approvals (Authorized to declare)	Actions	Timing	Communications	Resp. Group
Low	<ul style="list-style-type: none"> • Vulnerability difficult to exploit • Vulnerability can be easily blocked at entry. • Exploit requires physical access to a device. • Exploit requires user actions; e.g., going to a specific web site. • The payload is not destructive 	Technology Security	<ul style="list-style-type: none"> • Notification to all businesses and service providers • Testing and deployment included in next scheduled patch maintenance cycle 	<ul style="list-style-type: none"> • Based on applicable testing cycles. Start no later than 6 months from patch availability; finish no later than 12 months from start. 	<ul style="list-style-type: none"> • Notification to all businesses and service providers 	CIOs
Medium	<ul style="list-style-type: none"> • Vulnerability difficult to exploit • Existing controls make an attack unlikely • The exploit is not in the wild. • The exploit may affect important business applications or infrastructure, but the potential damage is limited. 	Technology Security	<ul style="list-style-type: none"> • Notification to all businesses and service providers • Testing and deployment included in next scheduled patch maintenance cycle 	<ul style="list-style-type: none"> • Begin action within 1 month of patch availability. • Complete patching within 6 months. 	<ul style="list-style-type: none"> • Notification to all businesses and service providers 	CIOs
High	<ul style="list-style-type: none"> • The vulnerability affects a large number of systems. • Vulnerability is easy to exploit • Existing controls may not adequately protect network. • Imminent exploit availability • Potential disruption is severe: e.g., data loss, network communication loss, impact on ability to conduct business. • An exploit could compromise key business systems or infrastructure. 	Head of the Information Security Office or their predefined delegates.	<p>Any one or more of the following, as needed:</p> <ul style="list-style-type: none"> • Block vulnerability at network perimeter: Internet, Extranet, Mail Gateways, IDS, and VPN, • Invoke predefined deployment plan. • Deploy AV signature files. • Business unit support groups accelerated patch testing • Scheduled BAU activity and deployments may be suspended. 	<ul style="list-style-type: none"> • Begin patching affected devices within 5 days of patch availability. • Complete patching within one month 	<ul style="list-style-type: none"> • ISO Notifies CIOs, BC Office. • Notification to all businesses and service providers 	CIOs
Critical	<ul style="list-style-type: none"> • The vulnerability affects a large number of systems. • Vulnerability easy to exploit • Existing controls may not adequately protect network. • Company is under attack or in imminent danger of being attacked; i.e., the exploit is “in the wild”. • Disruption or potential disruption is severe: e.g., data loss, network communication loss, impact ability to conduct business. • The virus or potential virus can propagate without user action. • Industry (vendor, security advisors, Homeland Security) recommends immediate action. 	Corporate CIO, or predefined delegates	<p>Take immediate action to mitigate risk to company. Actions may include:</p> <ul style="list-style-type: none"> • Block vulnerability at network perimeter: Internet, Extranet, Mail Gateways, IDS, and VPN. • Deploy AV signature files. • Patch affected devices. • Deny any vulnerable devices access to network. • Isolate impacted parts of the network. • Suspend scheduled BAU activity and deployments. 	<ul style="list-style-type: none"> • Begin action steps immediately. • Complete patching vulnerable machines as quickly as possible, but no later than 1 week from patch availability (Machines incapable of being patched addressed based on risk.) 	<ul style="list-style-type: none"> • ISO sends informational communication to CIOs, • ISO sends information communication to all associates • BC communication/ process activated (only if operational impact to business) • Notification to all businesses and service providers 	Tech Service Org

Appendix: C – Roles and Responsibilities Example

Users – Ensure their home systems maintain the most current anti-virus, personal firewall software as well as ensuring their systems have the latest patches.

Developers/users who are responsible for managing their own devices on the network -- maintain the most current anti-virus as well as ensuring their systems have the latest patches.

Security Analysis – Receive alerts from external sources; perform initial risk assessment (including initial internal risk rating), forward alert onto potentially affected groups and response team as needed; review updates and communicate as needed to management and associates as needed.

Response Team – Subject matter expert performs a more detailed risk assessment (e.g., change internal risk rating as needed); evaluate potential number of devices affected; and assess mitigating controls.

Infrastructure Service Provider – Implement mitigating controls; test / plan for patch deployment; and communicate status.

Operation Center Problem Manager – Manage incident if vulnerability / exploit enters the internal network.

CISO/Head of Corp Tech Services – Approves internal risk rating of orange and the resources required to quickly patch effected devices.

CIO – Approves internal risk rating of red and the resources required to immediately patch effected devices.