# Vulnerability and Patch Management

|  |  |
| --- | --- |
| Revision | 1.0 |
| Approval | Pending |

Proactively manage the security and resiliency of organization systems by performing effective vulnerability and patch management.

#### Commentary

According to the FFIEC Architecture, Infrastructure, and Operations booklet:

"Vulnerability management is a process to continuously acquire, assess, and take action on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Part of vulnerability management is patch management. Patch management is the systematic notification, identification, deployment, installation, and verification of OS and application software code revisions."

The longer a vulnerability is allowed to exist, the greater likelihood it may be exploited by a malicious actor. However, if patches for the vulnerabilities are not implemented properly, systems and operations can be damaged or disrupted. As such, the vulnerability and patch management process is an important component of the organization's change management process and contributes to the organization's greater security posture.

To minimize the risks associated with vulnerability and patch management, the organization's process is comprised of three primary phases: monitor, identify, and remediate.

Examples of systems which should be updated as part of this process include the organization's core systems, digital banking systems, network components, email systems, ACH and wire transfer systems, remote deposit capture (RDC) systems, automated teller machines (ATMs), virtual machines, mobile devices, and employee workstations (e.g., desktops, laptops, etc.), including backup systems (e.g., systems in the organization's disaster recovery environment), as applicable.

For the purposes of this policy, the terms "patch," "update," and "upgrade" will be used interchangeably to mean the implementation of a code revision to software applications, operating systems (OS), drivers, firmware, etc.

#### Implementation

**Monitor**

Maintain awareness of vulnerabilities and patches by monitoring the following.

* Results of weekly vulnerability scans
* Vendor articles, newsletters, press releases, and user groups
* Vulnerability alerts from the following third parties:
	+ Cybersecurity and Infrastructure Security Agency (CISA)
	+ Federal Bureau of Investigation
	+ Financial Services Information Sharing and Analysis Center (FS-ISAC)
	+ National Institute of Standards and Technology (NIST)
* System alerts and notices
* Other online forums, news sites, and email lists

**Identify**

Based on results of monitoring, evaluate whether identified vulnerabilities apply to the organization's environment. For applicable vulnerabilities:

* Assess each vulnerability's severity level (i.e., critical, high, medium, and low) and the risk it presents to the organization.
* Verify the vulnerabilities were not exploited. If any were exploited, implement the organization's Incident Response Plan.
* Determine if a patch exists to remediate the vulnerability and proceed with remediation. If a patch does not exist:
	+ Determine if compensating controls are necessary to ensure the security of affected systems.
	+ Monitor for the availability of a patch.
	+ Proceed with remediation when one becomes available.

**Remediate**

Mitigate vulnerabilities by implementing patches in accordance with each vulnerability's severity level.

* **Critical:** Patch affected systems within 7 days.
* **High:** Patch affected systems within 14 days.
* **Medium:** Patch affected systems within 30 days.
* **Low:** Patch affected systems within 90 days.

Implement patches in accordance with the organization's change management process, which is addressed in a separate policy (see the Related Policies section for additional information). Consider the following:

* Obtain patches only from authorized and trusted sources.
* Plan to install patches in a manner which causes minimal disruption for customers and personnel. Consider implementing a temporary freeze change prior to times of projected high use or limited staffing (e.g., holidays).
* Perform a data backup prior to installing a patch, as needed.
* Demonstrate extra care when installing patches on systems with unique configurations.
* Apply patches to a test environment prior to installing patches on a production environment.
	+ If the test is successful, consider installation of the patch for a broader test group, depending on the risk associated with the change.
	+ Verify tested patches did not introduce new vulnerabilities, reintroduce old vulnerabilities, degrade system performance, or alter system configurations.
	+ If a required patch fails testing and/or cannot be implemented in accordance with this policy, document a formal exception.

To implement patches:

* **For Microsoft systems,** use Windows Server Update Service (WSUS) / Windows Update / a third-party solution to keep systems up to date.
* **For non-Microsoft systems,** review all updates for other applications, such as core services, banking applications (e.g., loan processing, teller operations, etc.), and other software (e.g., Adobe, Java, web browsers, etc.).
* **For systems managed by a vendor,** ensure vendors install patches on the systems they maintain on behalf of the organization, as well as those which connect to the organization's network (e.g., digital banking, ATMs, cloud systems, etc.).

Log patch installations for all servers, routers, and other key network components.

Communicate with personnel regarding any actions they may need to perform to install a patch.

Consider blocking network connection attempts from unpatched systems.

#### Implementation Responsibility

* Network Administrator

#### Related Policies

| Related Policy | Description |
| --- | --- |
| Change Management | Follow the change management process for planned, routine, and emergency changes related to vulnerability and patch management. |
| Data Backup | Perform a backup of data prior to installing a patch, as needed. |
| Incident Management | Implement the Incident Response Plan if exploited vulnerabilities are discovered. |
| Information Sharing and Regulatory Monitoring | Monitor or subscribe to a service that checks for known vulnerabilities in software applications and operating systems (OS). |
| IT Asset Management | Refer to the IT asset inventory to determine which systems need updated. Update the IT asset inventory following installation of patches, as needed. |
| Mobile Devices | Ensure mobile devices used to connect to the organization's network are patched. |
| Network Diagrams | Critical versions or service packs of some software need to be documented on network diagrams. |
| Remote Work | Ensure patches are applied to systems used for remote work. |
| Security Testing | Review results of vulnerability assessments on a regular basis. |
| Third-Party Secure Application Development | Ensure applications developed by third parties include a process for installing patches. |
| Vendor Management | Engage with vendors to maintain awareness of vulnerabilities in third-party systems. Ensure patches are applied to organization systems managed by vendors. |

#### Committee/Team Review Items

| Frequency | Responsibility | Description |
| --- | --- | --- |
| Semiannually | Security Committee | Review patch management reports to ensure procedures are working, as expected, and resolve identified issues. |