Patch Management Standard

Introduction

Patch management is a critical preventive measure designed to proactively counter the exploitation of vulnerabilities existing within the State of Oklahoma infrastructure. By taking a proactive approach to managing vulnerabilities, the state is able to reduce or eliminate the potential for exploitation and prevent the excessive time, effort and cost of responding to an incident after it has occurred.

Purpose

This document establishes the vulnerability and patch management standard for the State of Oklahoma. By applying security-related software or firmware updates (patches) to applicable IT systems, the expected result is reduced time and money spent dealing with exploits by reducing or eliminating the related vulnerability.

Standard

- All nonconsolidated agencies must assign a business owner responsible for patch management. OMES is responsible for patch management for all consolidated agencies.
- If patch management is outsourced, service level agreements must be in place addressing the requirements of this standard and outlining responsibilities for patching. If patching is the responsibility of the third party, agencies must verify the patches have been applied.
- Patching must include all application software. This includes enterprise applications, custom applications, commercial off-the-shelf applications, legacy applications and all related software such as operating systems, virtualization, database, etc.
- A process must be in place to manage patches. This process must include the following:
    - Monitoring security sources for vulnerabilities, patch and nonpatch remediation and emerging threats. Example security sources are vendor website or notification lists, vulnerability scanners, penetration tests and the National Vulnerability Database.
    - Overseeing patch distribution, including verifying a change control procedure is followed.
    - Testing for stability and deploying patches.
    - Using an automated centralized patch management distribution tool whenever technically feasible. The tool should maintain a database of patches, deploy patches to endpoints and verify the installation of patches.
- Appropriate separation of duties must exist so that the individual(s) verifying patch distribution is not the same individual(s) distributing the patches.
- As per the Information Security Policy Procedures and Guidelines policy, all agencies must maintain an inventory of hardware and software assets. Patch management must incorporate all installed IT assets.
- Patch management must be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System and CISA directives. A CVSS score of 7-10 is considered a high-impact vulnerability, while 4-6.9 is considered a moderate-impact vulnerability and 0-3.9 is considered a low-impact vulnerability. A CISA directive is considered a critical-impact vulnerability.

- The patching process must follow the timeline shown here:

Impact/Severity	Patch Initiated	Patch Completed
Critical	Within **24 hours** of patch release.	Within **1 week** of patch release.
High	Within **24-72 hours** of patch detected in vulnerability management software.	Within **2 weeks** of patch detection.
Medium	Within **1 week** of patch release detected in vulnerability management software.	Within **1 month** of patch detection.
Low	Within **1 month** of patch release detected in vulnerability management software.	Within **365 days** during normal maintenance cycles unless ISO determines this an insignificant risk to environment.

- If patching cannot be completed in the specified timeframe, an extension must be requested from the chief information officer and the chief information security officer. The extension request must include:
    a. Detailed explanation of why the patching cannot be completed in the timeframe listed.
    b. List of compensating controls put in place.
    c. Remediation plan for getting the system(s) compliant with specified timeframe(s).

    Note: Any system that is noncompliant for more than two periods annually is subject to decommissioning.
- If a patch requires a reboot for installation, the reboot must occur within the specified timeframe.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- National Institute of Standards and Technology Special Publications: NIST 800-40.
- Common Vulnerability Scoring System.
- State of Oklahoma Security Policy, Procedures, Guidelines.
- Internal – 06.03.01 Change Management Process SOP.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 09/28/2021	**Review cycle:** Annual
Last revised: 10/20/2022	**Last reviewed:** 08/30/2023
Approved by: Joe McIntosh, Chief Information Officer	