NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	**No:** NYS-S15-001
IT Standard: **Patch Management**	**Updated:** 05/19/2021
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

Security patch management (patch management) is a practice designed to proactively prevent the exploitation of Information Technology (IT) vulnerabilities that exist within an organization. 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.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. Section 2 of Executive Order No. 117, established January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols, and standards for State government, including hardware, software, security, and business re-engineering. Details regarding this authority can be found in New York State (NYS) ITS Policy, *NYS-P08-002 Authority to Establish Enterprise Information Technology (IT) Policies, Standards and Guidelines*.

3.0 Scope

This standard applies to all “State Entities” (SE), defined as “State Government” entities in Executive Order 117, established January 2002, or “State Agencies” as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any ITS resource for which ITS or the SE has administrative responsibility, including

systems managed or hosted by third parties on behalf of ITS or the SE. While an SE may adopt a different standard, it must include the requirements set forth in this one.

This standard is applicable to all systems owned or operated by, or on behalf of, NYS.

This standard relates specifically to vulnerabilities that can be addressed by a software or firmware update (patch) and applies to all software used on NYS systems. The NYS-S15-002 Vulnerability Scanning Standard should be followed for requirements on addressing non-patched vulnerabilities.

4.0 Information Statement

1. State entities (SE) are responsible to ensure an individual or group is overseeing patch management for any given system. That individual or group may be within IT operations.

2. If patch management is outsourced, service level agreements must be in place that address the requirements of this standard and outline responsibilities for patching. If patching is the responsibility of the third party, SEs must verify that the patches have been applied.

3. A process must be in place to manage patches. This process must include the following:

    - Monitoring security sources (Exhibit 1) for vulnerabilities, patch and non-patch remediation, and emerging threats.
    - Overseeing patch distribution, including verifying that a change control procedure is being followed.
    - Testing for stability and deploying patches.
    - Using an automated centralized patch management distribution tool, whenever technically feasible, which
        - Maintains a database of patches.
        - Deploys patches to endpoints.
        - Verifies installation of patches.

4. Appropriate separation of duties must exist so that the individual(s) verifying patch distribution is not the same individual(s) who is distributing the patches.

5. As per the NYS-P03-002 Information Security Policy, all SEs must maintain an inventory of hardware and software assets. Patch management must incorporate all the SE's installed IT assets.

6. Patch management must be prioritized based on the severity of the vulnerability that the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System (CVSS) v3.0 Ratings. A CVSS score of 9.0-10.0 is a critical vulnerability; 7.0-8.9 is a high impact vulnerability; a score of 4.0-6.9 is a moderate vulnerability; and a CVSS of 0.1-3.9 is considered a low impact vulnerability.

7. The NYS Chief Information Security Office (CISO) may deem any vulnerability to be high impact, regardless of CVSS score, based on a NYS specific analysis.

8. The impact to the SE's information assets is based on the asset's information classification as per the NYS-S14-002 Information Classification Standard. To the extent possible, the patching process must follow the timeline contained in the tables below:

Table 1: RISK RATING			
Impact (Confidentiality, Integrity, Availability)	**Exposure**		
	Systems with no network connectivity to production data	**Systems with network connectivity to production data (not internet facing)**	**System that is publicly available from the internet**
High	**Moderate**	**High**	**High**
Moderate	**Low**	**Moderate**	**High**
Low	**Low**	**Low**	**High**

TABLE 2: PATCH TIMEFRAMES				
Vulnerability Severity				
Risk Rating (from Table 1)	**Critical**	**High**	**Moderate**	**Low**
High	15 calendar days	30 calendar days	3 months	At the discretion of the ISO/designated security representative
Moderate	30 calendar days	3 months	6 months	At the discretion of the ISO/designated security representative
Low	4 months	6 months	At the discretion of the ISO/designated security representative	At the discretion of the ISO/designated security representative

9. If patching cannot be completed in the timeframe listed in the table above, compensating controls must be put in place within the timeframes above and the exception process must be followed.

10. If a patch requires a reboot for installation, the reboot must occur within the timeframes outlined above.

5.0 Compliance

This standard shall take effect upon publication. Compliance is required with all ITS policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities shall request an exception through the Chief Information Security Office exception process.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-S15-001
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This policy document should be reviewed consistent with the requirements set forth in *NYS-P09-003 Process for Establishing Information Technology Policies, Standards, and Guidelines*

Date	Description of Change	Reviewer
01/16/2015	Original Standard Release	Deborah A. Snyder, Deputy Chief Information Security Officer
02/25/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
09/11/2018	Scheduled review – minor changes to Authority, Scope, and title of office	Deborah A. Snyder, Chief Information Security Officer
05/04/2021	Updated impact and patch timeframes based on Federal guidance.	Karen Sorady, Chief Information Security Officer
05/19/2021	Updated Scope language	Karen Sorady, Chief Information Security Officer

9.0 Related Documents

National Institute of Standards and Technology, Special Publication 800-40, Guide to Enterprise Patch Management Technologies

Common Vulnerability Scoring System

National Vulnerability Database Vulnerability Severity Rankings

Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 19-02

NYS-S15-002 Vulnerability Management Standard

Exhibit 1: SAMPLE SECURITY SOURCES FOR VULNERABILITY/PATCH/THREAT INFORMATION

- NYS Cyber Security Operations Center (includes feeds from US-CERT, NCCIC, and MS-ISAC)
- Vendor websites/notification lists
- BugTraq
- Vulnerability Scanners
- Penetration Tests
- National Vulnerability Database