



New York State Information Technology Standard	No: NYS-S15-001
IT Standard: Patch Management	Effective: 01/16/2015
	Issued By: NYS ITS Standard Owner: Enterprise Information Security Office

1.0 Purpose and Benefits of the Standard

Security patch management (patch management) is a practice designed to proactively prevent the exploitation of 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 Enterprise IT Policy/Standard Statement

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), 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 NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

3.0 Scope

This standard is applicable to all systems owned and/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 Vulnerability Scanning Standard](#) should be followed for requirements on addressing non-patched vulnerabilities.

4.0 Information Statement

- 4.1. State entities (SE) must assign an individual or group within IT operations to be responsible for patch management.
- 4.2. 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.
- 4.3. A process must be in place to manage patches. This process must include the following:
 - monitoring security sources ([Appendix A](#)) 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; and
 - using an automated centralized patch management distribution tool, whenever technically feasible, which:
 - maintains a database of patches;
 - deploys patches to endpoints; and
 - verifies installation of patches.
- 4.4. 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.
- 4.5. As per the [NYS Information Security Policy](#), all SEs must maintain an inventory of hardware and software assets. Patch management must incorporate all of the SEs installed IT assets.
- 4.6. 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 (CVSS). A CVSS score of 7-10 is considered a high impact vulnerability, a CVSS score of 4-6.9 is considered a moderate impact vulnerability and a CVSS of 0-3.9 is considered a low impact vulnerability.
- 4.7. Vulnerability advisories from the NYS ITS Enterprise Information Security Office (EISO) Cyber Security Operations Center (CSOC) are based on a NYS specific analysis of impact and must be considered high impact vulnerabilities, regardless of CVSS score.
- 4.8. To the extent possible, the patching process must follow the timeline contained in the table below:

Impact/Severity	Patch Initiated	Patch Completed
High	Within 24 hours of patch release	Within 1 week of patch release
Medium	Within 1 week of patch release	Within 1 month of patch release
Low	Within 1 month of patch release	Within 2 months of patch release, unless ISO determines this to be an insignificant risk to the environment

- 4.9. 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.
- 4.10. 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. The Policy Unit shall review the standard at least once every year to ensure relevancy. The Office may also assess agency compliance with this standard. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, SEs shall request an exception through the Enterprise Information Security Office [exception process](#).

6.0 Definitions of Key Terms

Not applicable

7.0 ITS Contact Information

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

Standard Owner
Attention: Enterprise Information Security Office
New York State Office of Information Technology Services
1220 Washington Avenue – Bldg. 7A, 4th Floor
Albany, NY 12242
Telephone: (518) 242-5200
Facsimile: (518) 322-4976

Questions may also be directed to your ITS Customer Relations Manager at:
Customer.Relations@its.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

8.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
01/16/2015	Original Standard Release	Deborah A. Snyder, Deputy Chief Information Security Officer
01/16/2016	Scheduled Standard Review	

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](#)
- [NYS Vulnerability Scanning Standard](#)

Appendix A: 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](#)