

AHS Flaw Remediation Standard

Jack Green

10/14/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the System Monitoring (SI-1, SI-2, SI-2(1), SI-2(2)) Controls.

Revision History

Date	Version	Description	Author
	.99	Draft received from HI and reviewed by Referentia	
	1.0	Created Document	AHS
8/16/2013	2.0	Document revised for VHC standards	Jack Green
10/14/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements	Jack Green

PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the System Monitoring (SI-1, SI-2, SI-2(1), SI-2(2)) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

SCOPE

The scope of this standard includes the VHC and its constituent systems only

STANDARD

Flaw Remediation

1. The VHS shall identify, report, and correct information system flaws.
2. An inventory of information systems and components must be collected and maintained in order to determine which hardware equipment, operating systems, and software applications are in operation.
 - The inventory, both for the enterprise and at each office and region, must include both standard information systems and components and those not designated as organization standards (i.e., non-standard equipment, operating systems, and software applications).
 - All software monitored, including the vendor, version, and support contract information, must be part of the inventory. Software types include:
 - i. Firmware.
 - ii. Commercial-Off-the-Shelf (COTS).
 - iii. Government-Off-the-Shelf (GOTS).
 - iv. Operating System, to include computer and network operating systems.
 - v. Standard applications.
 - vi. Custom applications.

3. Flaw remediation must be incorporated into VHC's configuration management process.
4. A Patch and Vulnerability Management Plan must be developed as part of the Configuration Management Plan and must address the following:
 - All equipment, operating systems, and software applications must be included.
 - The criteria for implementing flaw remediation's must be defined with respect to:
 - i. Threat level.
 - ii. Risk of compromise.
 - iii. Consequences of compromise.
 - The responsible party for monitoring and coordinating with each vendor for patch release support must be designated.
5. Information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) must be reported to designated organizational officials with information security responsibilities (e.g., Senior Information Security Officers, Information System Security Managers, Information Systems Security Officers).
6. Vulnerability and remediation information must be disseminated to local system administrators and security personnel.
 - Standard email distribution lists must be established.
7. System administrators must be instructed or trained on how to apply vulnerability and configuration management remediation.
 - Notifications of vulnerabilities and remediation's must contain instructions on how to apply them, if automated mechanisms are not used.
8. Vulnerabilities and remediation actions must be prioritized, and their priority order must be based on the individual vulnerability criticality or severity ratings.
 - Priorities must be established based on the source's assessment of severity or criticality as high, moderate/medium, or low.
 - The next highest priority available from the following sources must be used unless the VHC has established a different priority:
 - i. Vendor web sites and mailing lists.
 - ii. Third-party web sites.
 - iii. Vulnerability scanner.
 - iv. Vulnerability databases.
 - v. Enterprise patch management tools.
 - vi. Other notification tools.
 - Source severity assessments other than those established by US-CERT may be modified in accordance with detailed knowledge of criteria specific to the Organization, by using NIST's CVSS Calculator, provided the criteria, ratings,

and results are documented and retained for the record and the alteration is noted in the alert.

- NIST's CVSS Calculator must be used to establish priority as follows:
 - i. Vulnerabilities must be labeled "Low" severity if they have a CVSS base score of 0.0–3.9.
 - ii. Vulnerabilities must be labeled "Medium" severity if they have a base CVSS score of 4.0–6.9.
 - iii. Vulnerabilities must be labeled "High" or "Critical" severity if they have a CVSS base score of 7.0–10.0.
9. A database of remedial actions that need to be applied to the organization's IT resources must be created and maintained.
- Vulnerability remediation must be monitored.
10. Software updates related to flaw remediation, (including patches, services packs, and hot fixes) must be tested before installation for effectiveness and potential side effects on VHC information systems.
- The level and timing of testing may vary and depend on risk to the information system and priority of the remediation.
 - i. Fixes for vulnerabilities ranked high or critical must be tested as soon as possible but no later than two business days.
 - ii. Fixes for vulnerabilities ranked moderate or medium must be tested within seven business days.
 - iii. Complete testing of fixes for low priority vulnerabilities must be completed within 30 days.
 - Existing change management procedures must be used for testing low priority remedial actions and, when possible, for testing patches and configuration modifications of moderate/medium priority vulnerabilities.
 - The flaw remediation process must be centrally managed and software updates must be installed automatically.
 - The software code for all patches, service packs, hot fixes, etc., must be verified before testing or installation.
 - i. A vendor authentication mechanism (e.g., cryptographic checksums, Pretty Good Privacy [PGP] signatures, digital certificates) must be used to ensure the authenticity of the code.
 - a. SHA-1 checksums from vendors must be used, instead of MD5 or similar checksums, whenever they are available.
 - ii. The code must be scanned for viruses using the most current virus signature database.
 - iii. A search must be performed to learn what experiences others have had in installing or using the patch.

- All remediation changes must be tested on non-production systems prior to implementation on all organization-standard IT products and configurations in order to reduce or eliminate the following:
 - i. Unintended consequences.
 - ii. Alteration of security settings.
 - iii. Enabling of default user accounts that had been disabled.
 - iv. Resetting of default passwords for user accounts.
 - v. Enabling of services and functions that had been disabled.
 - vi. Non-security changes, such as new functionality.
- Testing of patches must ensure that patches are installed in the required sequence and any removal of any previous security patch is not unintended.
- Testing must include checking all related software to ensure that it is operating correctly.
- Testing must include a selection of systems that accurately represent the configuration of the systems in deployment.
 - i. Testing of remedial actions must be conducted on IT components that use standardized configurations.
 - a. Images of standard configurations must be used on test systems or within virtual machines on test systems that can expedite the testing process.
 - ii. Non-standard IT products that have been approved for use within the VHC must be tested using approved configurations.

11. Based on the results of testing, it must be considered whether any significant disadvantages outweigh the benefits of installing a patch and whether remediation should be delayed.

- If the potential negative consequences are significant, then the following must be considered:
 - i. Waiting until the vendor releases a newer patch that corrects the major issues.
 - ii. The ability to “undo” or uninstall a patch.
- Delay of high or moderate/medium priority remediation must be approved by the Senior Agency Information Security Officer, (SAISO) with appropriate documentation of rationale and mitigation measures.

12. A schedule for the release and implementation of patches, service packs, and hot fixes for Organization-standard configurations must be developed by the SAISO, as needed, in coordination with CSIRC, and individual system security personnel.

- The patch release schedule must be developed using a risk-based decision that is in compliance with pre-defined criteria (i.e., threat level, risk of compromise, and consequences of compromise) outlined in the Flaw and Vulnerability Management Plan.

13. Security-relevant software updates (e.g., patches, service packs, and hot fixes) must be installed promptly by VHC and any VHC contractors.

- The requirements for testing and consideration of significant negative consequences of the remediation must still apply.
- Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.
- The priority of the vulnerability must determine how promptly the remediation is implemented.
 - i. Vulnerabilities ranked high or critical must be mitigated and reported to CSIRC within two business days after testing is completed.
 - ii. Vulnerabilities ranked moderate/medium must be mitigated and reported to CSIRC within seven business days after testing is completed.
 - iii. Vulnerabilities ranked low must be mitigated within 30 days.
- Automated deployment of patches to IT devices using enterprise patch management tools must be performed.
 - i. VHC's standard tools for automated patch deployment and installation must be used.
 - ii. When automated mechanisms are not available, feasible, or appropriate, manual patch installation and remediation must be performed.
- Automated tools acquired to support vulnerability and configuration management remediation actions must be selected based on the following order of priority:
 - i. Tools that implement, support, and are validated by NIST to conform to the Security Content Automation Protocol (SCAP)
 - ii. Tools that are pursuing or have a corporate commitment to conformance with NIST validation of SCAP
 - iii. Tools that readily integrate with other SCAP-validated tools
 - iv. Commercial tools that lack SCAP validation, in the absence of validated tools
 - v. Tools developed in house that readily integrate with SCAP-validated tools

14. Vulnerability and flaw remediation actions must be tracked and verified.

- Appropriate automated tools and methods include, but are not limited to, the following:
 - i. Patch deployment tool database
 - ii. Network and host vulnerability scanning
 - iii. Configuration management tool

- Where automated tools are not feasible, installation must be verified by manual methods, including, but not limited to the following:
 - i. Inspecting the configuration, operating system, or application.
 - ii. Reviewing files or configuration settings that the remediation was intended to correct to ensure that they have been changed as stated in the vendor's documentation or instructions.
 - a. This may or may not be a function of the tool used.
 - iii. Reviewing patch logs
 - Verification must not employ exploit procedures (e.g., a penetration test) or code to exploit any vulnerability without written authorization and approval from the information system's Authorizing Official (AO).
 - i. Exploit methods such as penetration testing may be used without authorization and approval only on test systems in a test environment.
 - The accomplishment of procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts must be verified.
15. When flaw remediation and vulnerability mitigation activities are completed, the following actions must occur:
- The inventory of information systems and components must be updated to reflect current software versions and configurations.
 - Stakeholders, including but not limited to VHC's Computer Security Incident Response Capability (CSIRC), must be notified.
 - Reporting to CSIRC must be via the VHC incident reporting system, unless status is available through an automated tool visible to CSIRC personnel.
 - NIST SP 800-40, Version 2.0 must be used as guidance on security patch installation and patch management.

IMPORTANT INFORMATION

These procedures can be found at <http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec>