

AHS Vulnerability Scanning Standard

Jack Green

10/17/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Vulnerability Scanning (RA-1, RA-5, RA-5(1)) 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
10/17/2013	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 Vermont Health Connect's (VHC) security control requirements for the Vulnerability Scanning (RA-1, RA-5, RA-5(1)) 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

Vulnerability Scanning

1. Prior to commencing vulnerability scanning efforts, the following should be addressed:
 - i. Scanner selection – SOs shall evaluate the tools for use within their respective environments.
 1. The network and host-based vulnerability scanner must provide the following capabilities:
 - a. Identify active hosts on networks.
 - b. Identify active and vulnerable services (ports) on hosts.
 - c. Identify vulnerabilities associated with discovered operating systems and applications.
 2. The VHC shall implement a suite of automated monitoring tools to more effectively monitor and identify vulnerabilities on networked computer servers.
 - ii. Purpose – A vulnerability scan must have a defined purpose. Vulnerability scanning happens periodically, as part of the information system authorization process, and during the risk assessment process.
 - iii. Vulnerability scans are typically performed against all systems and for all known vulnerabilities.

- iv. The SO shall conduct vulnerability scans to be performed as noted below:
 1. Regularly scheduled scans must occur at most every 30 days.
 2. Additional scheduled scans must occur after system updates or the identification of a major vulnerability.
 3. Unscheduled scans may occur when deemed necessary by the ISSO.
 - v. Scope/boundaries – An active vulnerability scan must have a defined scope or boundary.
 - vi. The scope must be clearly defined in written Rules of Engagement (ROE).
 - vii. The scan must be limited to a specific information system, system(s), subnet(s), or network(s) within the realm of responsibility for the VHC.
 1. If scans will occur outside the realm of responsibility for the VHC, then a memorandum of understanding (MOU) must be drafted and signed by the AO of each affected Agency.
 - viii. Signatures/tests – Compliance with the VHC's configuration standards must be tested. The signatures/tests that will be run against identified scope/boundaries should be selected as appropriate for the purpose of the vulnerability scanning.
 - ix. Research potential negative impacts – Once signatures/tests are selected, research should occur to determine if any of those signatures/tests may have a potential negative impact on the scope/boundaries selected.
2. Coordination/announcement – Coordination with and/or notification to the relevant or affected parties, depending on the scope and purpose of the scans, must occur before an active vulnerability scan is performed, especially if that scan may result in a potential negative impact.
 3. The VHC shall scan for vulnerabilities in the information system and hosted applications at least every 90 days for a system with a low system categorization.
 4. High and Moderate systems shall be scanned weekly and when new vulnerabilities potentially affecting the system/applications are identified and reported.
 - i. The security categorization of the information system must guide the frequency and comprehensiveness of the vulnerability scans.
 - ii. Vulnerability scanning must include scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.
 - iii. The information system vulnerabilities list shall be updated at least weekly or when new vulnerabilities are released.
 5. Vulnerability scanning and penetration testing must be used to assess the adequacy of security controls for the information system and adherence to federal and Agency requirements.

6. The VHC shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.
7. Vulnerability scan reports and results from security control assessments must be analyzed.
8. External testing must be performed by a recognized independent security resource.
 - i. Testing must, at a minimum, include remote scanning and probing to identify potential exploits and vulnerabilities.
 - ii. Test results must capture all vulnerabilities and must include recommendations for implementing industry best practices solutions.
 - iii. Testing must be conducted on specifically identified assets with the advice and consent of the CIO.
9. Vulnerability scanning must be conducted using scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards that:
 - i. Enumerate platforms, software flaws, and improper configurations.
 - ii. Format and make transparent, checklists and test procedures.
 - iii. Measure vulnerability impact.
10. Vulnerability scans must have defined a clear scope for all vulnerability scanning activities and designate knowledgeable and trained individuals to perform the scans.
11. The following must be addressed before, during, and after the vulnerability scan:
 - i. Update scanning software – Before the vulnerability scan is performed, the vulnerability scanner must be updated with the latest patches and database signatures/tests. Scanners that are not maintained and out of date will not contain the most recent signatures/tests and, as a result, vulnerabilities could be missed. Scans performed by scanners that are not maintained are not valid for meeting the scanning requirements and results cannot be claimed on FISMA reporting or used in the security assessment and authorization process.
 - ii. Perform scanning exercise – The designated personnel shall perform the scan of the network and devices in accordance with the established ROE.
 - iii. Verify system availability – After completing the test, the designated personnel shall check system status directly or by coordinating with the system administration team to ensure that the test did not result in unintended consequences and that the system remains operational.
12. Once the vulnerability scanning has been completed, the results must be analyzed and documented in a vulnerability scan report.
13. The Program Manager shall review, approve, and sign all custom-developed code prior to deployment into production environments.
 - i. The Program Manager may delegate this authority to another VHC employee in writing.

- ii. This authority shall not be delegated to contractor personnel.
14. Discovered deficiencies must be added to the system POA&M for correction or mitigation as follows:
- i. Critical or High Vulnerabilities – These must be reported immediately when verified.
 - 1. SOs shall have 30 days to correct these after which a POA&M must be established.
 - ii. Moderate Vulnerabilities – These must be corrected within 60 days after which a POA&M must be established.
 - iii. Low Vulnerabilities – These must be corrected after high and moderate vulnerabilities are corrected as time permits. POA&Ms do not need to be established unless an aggregation of these vulnerabilities raises the risk to moderate or high.
15. The following corrective actions must be employed when necessary as a result of scanning for vulnerabilities:
- i. Upgrade or patch vulnerable systems to mitigate identified vulnerabilities as appropriate.
 - ii. Deploy mitigating measures (e.g., management, technical, procedural) if the system cannot be immediately patched.
 - iii. Improve the change management and configuration management program and procedures and standards to ensure that systems are upgraded routinely with the latest solutions.
 - iv. Assign a specified team or person(s) responsible for monitoring vulnerability alerts and mailing lists, examine applicability to the Agency's environment, and initiate appropriate system changes.
16. Modify or recommend modifications to the Agency's security policies, architecture, or other documentation, processes or procedures to ensure that security practices include timely system updates and upgrades.

IMPORTANT INFORMATION

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