VistA National Patch Release Requirements

Department of Veterans Affairs

Office of Information and Technology (OIT)

March 2022

Version 1.0

Revision History

Date	Version	Description	Author
03/31/2022	1.0	Initial Version	VistA Office

Table of Contents

VistA National Patch Release Requirements

1. Introduction

The purpose of the Veterans Health Information Systems and Technology Architecture (VistA) National Patch Release Requirements information in this guide, is to call attention to the importance of following and completing all the steps in the VistA patch release process. The VistA National Patch Module Guide (NPMG) is the authoritative source and provides the necessary information to initiate, develop, create, and release patches to VistA products. VistA patch products consists of both Mumps and non-Mumps software code, that affect systems inside and outside of the VistA authorization boundary, therefore collaboration is essential to provide support to all consumers of VistA software.

Product staff that contribute to the release of a VistA Patch are comprised of both VA and contractor personnel assigned to various organizational elements. VistA patch releases are managed as national releases, however, there is not a standard change management process that is currently in use, therefore this creates potential security vulnerabilities within the VistA authorization boundary. This section reminds Product staff of key tasks and responsibilities within the VistA patch release process that must be properly executed to avoid security failures.

2. Processes

The VistA patch process is assessed by Information Assurance inspectors under the lens of the Configuration Management security control, with a specific focus on configuration and change control, access restrictions for change, and Information System Component inventory. These assessments review the practices from ensuring the enforcement of physical and logical changes in association with VistA are approved, to include providing an inventory of documentation associated with the release of VistA patches. The aim of this document is to eliminate the findings that are levied by security assessment teams when inspecting the VistA Change and Configuration Management process.

During various change and configuration management process assessments, the teams involved in the patch release process may be contacted to provide confirmation of the VistA patch release process. Contact will come in the form of request for evidence that include artifacts such as an initial ticket for change request, management approval documents, testing, and release information. By clearly identifying and understanding the roles and responsibilities of the product teams responsible for releasing VistA patches provides a means of coordination to answer any inquiries from the assessment team. Key members of the VistA patch release process are listed below.

1. The Team Leader will be responsible for the oversight and management of the patch development process as follows:
    - Project manager leads the team and is responsible for the patch

- Responsible for patch oversight management
- Identify personnel including roles and responsibilities
- Provide access to document repository
- Manage project and test site team calls

2. The Primary Developer will receive the assigned defect or enhancement, and perform the following tasks:

    - Receives assigned defect or enhancement notification
    - Creates patch stub in the NPM (Forum)
    - Coordinate routine conflicts (May encompass working with other developers to coordinate patch development/release process)
    - Inspect routines that overlap in patches, report findings
    - Follow the software development process
    - Unit testing
    - Create Patch Tracking Message
    - Coordinate IOC Testing
    - Coordinate patch completion with SQA Analyst and Verifier
    - For the VistA Primary Developer Review Checklist, please use this link:

      https://dvagov.sharepoint.com/:w:/r/sites/OITProcessAssetLibrary/_layouts/15/Doc.aspx?sourcedoc=%7BF7BF7860-545B-431A-9C31-49294AA95E29%7D&file=vista_primary_developer_review_checklist.docx&wdLOR=cDD71510F-65D9-46A4-883A-43883AA8A823&action=default&mobileredirect=true&cid=db7630d4-9618-4558-81fc-453504daf023

    The SQA Analyst is responsible for the following:

    - Ensuring policies, practices, and guidelines are followed in a project
    - Ensures the VistA SQA Checklist is completed for each test version reviewed
    - Coordinate patch completion with both the Developer and Verifier
    - Use the following link for the VistA SQA Checklist: https://dvagov.sharepoint.com/:x:/s/OITEPMOSoftwareTesting508/Ea95V9VHvNpIqXT1QMEemW0Bontu7quG0bpZEmNfBcVzCA?e=rf6idq

3. The Verifier is responsible for the following:
    - Responsible for assisting with the coordination with the patch release process
    - When applicable work with IOC test sites
    - Complete the verifier checklist
    - Coordinate with Developer and SQA on patch completion
    - Release the path and set the patch compliance date
    - When applicable move build/executables and documentation to the National File Server
    - Use the following link for the VistA Verifier Checklist:

https://dvagov.sharepoint.com/sites/OITProcessAssetLibrary/Library/vista_verifier_checklist.docx

3. Patch Release Gap Analysis

The following section outlines keys to successfully addressing change and configuration management artifact request during security assessments along with Office of Inspector General inspections.

- Documented standard change and configuration management process exist
- Primary contacts exist to represent the patch release project
- All members of the patch project team clearly recorded and identified
- All concurrences and approvals exist throughout patch lifecycle
- All release artifacts stored and available on demand by inspection teams

4. References

The National Patch Module Guide dated September 2021 is the source document used to develop the above information and is available at this link:

https://dvagov.sharepoint.com/:w:/r/sites/OITProcessAssetLibrary/_layouts/15/Doc.aspx?sourcedoc=%7B973F05BD-FD2F-4FE2-9825-CC92D965CA4D%7D&file=vista_national_patch_module_guide.docx&wdLOR=c8A66EC60-6917-498F-9F51-EF44AEEF5D77&action=default&mobileredirect=true&cid=4d8af30d-6986-40b8-933a-ce816e636aa3

5. Contact

For more information on VistA National Patch Release Requirements, please contact the VistA Process Governance Workgroup at VISTAProcessGovernanceWorkgroup@va.gov