Patch and Vulnerability Management Plan

12 Dec 2025

Authored By	Reece Niemuth
System Identifier	PCOS-Homelab
Date of Latest Revision	12 Dec 2025
Publication Version	Revision 1 (1.0.0)

CONTAINS NO CLASSIFIED OR SENSITIVE INFORMATION. THIS ARTIFACT SERVES TO DOCUMENT, IN PROFESSIONAL MANNER, A TRAINING RESOURCE FOR SELF-EDUCATION IN THE FIELD OF FEDERAL SYSTEMS ENGINEERING, MAINTENANCE, CYBERSECURITY RESEARCH, AND RELATED.

Patch and Vulnerability Management Plan : Revision History

Revision / Version	Date	Description / Notes
Rev. 1 (1.0.0)	12 Dec 2025	Publication Inception / Creation

1. Purpose

The purpose of this Patch and Vulnerability Management Plan is to define how the **Patriot Command Operations System (PCOS)** identifies, assesses, and remediates **software vulnerabilities and system flaws**. This plan ensures that known vulnerabilities are addressed in a **timely, disciplined, and documented manner**, while remaining practical for a single-operator laboratory environment.

2. Scope

This plan applies to all PCOS system components, including:

- Servers and workstations
- Virtual machines and hypervisors
- Network and security devices
- Supporting infrastructure and services

It covers:

- Operating system patches
- Application updates
- Security-related configuration fixes

3. Vulnerability Identification

Vulnerabilities within PCOS are identified through multiple sources, including:

- **Authenticated and unauthenticated vulnerability scans** using Nessus
- **Compliance and configuration findings** from SCAP and STIG-based assessments
- System monitoring, log review, and manual inspection
- Vendor security advisories and update notifications

Findings from **Nessus scans** and **SCAP/STIG compliance scans** serve as the primary drivers for remediation activity.

4. Assessment and Prioritization

Identified vulnerabilities are evaluated to determine:

- Severity and exploitability
- Potential impact to confidentiality, integrity, or availability
- System role and exposure

Given the limited scale of PCOS, prioritization is pragmatic and focuses on:

- High and critical findings first
- Issues affecting externally exposed or security-relevant systems
- Vulnerabilities with known exploits

Not all findings require immediate remediation; some may be addressed during scheduled maintenance or documented as accepted risk.

5. Remediation and Patching

Remediation actions may include:

- Applying operating system or application patches
- Updating vulnerable services or libraries
- Modifying insecure configurations
- Removing unnecessary or vulnerable software

Patching is performed using vendor-supported update mechanisms or trusted repositories.

All **flaw remediation and patching efforts** are documented in the **PCOS Change, Version, and Maintenance Log**, including:

- Description of the vulnerability or finding
- Action taken
- Date of remediation
- Affected system(s)

6. Validation and Documentation

After remediation:

- Systems may be rescanned using Nessus or SCAP/STIG tools to confirm resolution
- Configuration changes are reviewed to ensure stability and security
- Relevant documentation is updated as needed

Documentation serves as evidence of **continuous improvement and system hygiene**, rather than formal compliance reporting.

7. Review and Maintenance

Patch and vulnerability management activities are conducted:

- Periodically, based on system availability and time constraints
- Following significant system changes
- In response to high-risk findings

PCOS is a **non-regulated, single-operator environment**; therefore, remediation timelines are flexible and focused on **risk reduction and learning**, not strict regulatory deadlines.

See Change Log for Historical Record of Patching and Flaw Remediation