ACHE Vulnerability and Patch Management Standard

Document Name: ACHE Vulnerability and Patch Management Standard
Version: 1.0
Accountable: Alex Withers
Authors: Alex Withers

Reviewed: June 24, 2021
Approved: August 12, 2021 by IIB

Introduction

Vulnerability management is a key component to the protection and maintenance of any modern compute system. NCSA policy requires all systems with high risk data to have a plan to identify and remediate security vulnerabilities. This standard sets describes how system's vulnerabilities are managed in the context of the regular patching and maintenance of systems in the Advanced Computational Health Enclave (ACHE).

Supporting Policies & References

There are several supporting policies, standards and guides, some of which include:

- NCSA Information Security Policy
- NCSA Network Security Policy
- Understanding Severities in the SECURITY JIRA Queue
- ACHE Change Control Process

Scope

This standard applies to all systems in the NCSA's Advanced Computational Health Enclave where there is not a more specific system-level standard. It includes any hardware dedicated to ACHE, including switches, hypervisors, and support systems as applicable. Exceptions are made for devices that cannot be scanned or updated.

Vulnerability Identification

Vulnerability identification includes scanning all critical systems and a representative cluster member weekly. Two types of scans are utilized: perimeter scans and authenticated scans. Perimeter scans probe the services (from non-NCSA IP addresses when possible, local appliances when not) without logging in. Authenticated scans are performed from local appliances that authenticate to the systems using restricted non-root privileged accounts that query the system for information such as kernel and installed packages versions. A continuously updated vulnerability analysis tool uses this information to generate reports for consumption by both systems administrators and security team members.

The reports are discussed at regularly occurring meetings between the Systems and Security teams. These meetings are also used to discuss other intelligence gathered by the NCSA security team; such as information gathered through threat hunting, other security intelligence gathering systems and any vendor or community provided notices and intelligence. Items that require action on the part of the Systems Team are communicated via the NCSA ticketing system. High priority items are also followed up directly with a system administrator and with management.

Major configuration changes or the addition of services require a vetting of the changed system and services by the NCSA Security team. The Security team reviews the configuration for adherence to best practices and runs vulnerability scanning tools against the changed service.

Vulnerability Response

Standard Updates

Standard patches are performed during regular **quarterly** outages and include basic OS updates (including security patches) and other updates from vendors. A full vulnerability scan is performed again after any of these planned maintenances (PM).

These quarterly PMs are generally done during weekends and off hours with prep work to minimize customer downtime. However, they may can require a full service outage.

Urgent Updates

Urgent patches could be from a **critical** (See Understanding Severities in the SECURITY JIRA Queue) security vulnerability that cannot be mitigated or for something that destabilizes the system or a subcomponent. After install the efficacy of the changes are tested.

When possible these are done in a rolling update to avoid complete system outages, but it can require and entire unplanned outage. In these cases customers are promptly notified of the plan, and the outage will be posted on the NCSA service status page unless further discretion is required by the customer.

Special Requests

Customers may have special requests for new features, service or updated packages or libraries. Any change must go through the ACHE change control process for the ACHE. Minor changes, updates, requests, etc. can be captured as a standard change under the ACHE change control process to make these requests more efficient.