NCSA Vulnerability Management Policy

Document Name: NCSA Vulnerability Management Policy
Version: 1.2
Accountable: CISO (James Eyrich)
Authors: Alex Withers

Reviewed: August 22, 2023
Approved: IIB approved April 6, 2023

Scope and Purpose

This standard applies to all systems and networks within NCSA's control and ownership where there is not a more specific system-level standard. Exceptions can be requested for devices that cannot be scanned or updated. Note that for end of life or support operating systems (OS) an exception must include a concrete plan for an OS upgrade or decommissioning. NCSA policy requires all systems to have a plan to identify and remediate security vulnerabilities.

In addition to the use of automated tools for vulnerability management of externally-exposed and internal assets, the NCSA Security Office performs active vulnerability discovery to detect misconfigurations, systems, applications and networks that are not compliant with University policies, and general cyber weaknesses. The goals of this program are to detect issues more broadly for all NCSA cyber-infrastructure and to investigate more deeply than simple checklists for NCSA's most critical infrastructure.

Vulnerability Identification

The NCSA Security Office performs vulnerability scanning on NCSA cyberinfrastructure assets. Discovered vulnerabilities are investigated, categorized and documented in NCSA's ticketing system for remediation. These vulnerabilities are discussed between the NCSA Security Office and system owners and/or system managers during regular meetings.

Vulnerability Management

Vulnerabilities must be acknowledged and a remediation plan made according to the severity of the vulnerability and criticality of the asset. For all NCSA assets it is required by NCSA policy that detected vulnerabilities are remediated and that the NCSA Security Office is granted access for authenticated and non-authenticated vulnerability scans and to manually verify vulnerabilities.

NCSA must be able to identify the assets on which the vulnerability was found and who is responsible for those assets. Such data is normally acquired through the NCSA system vetting process. Additionally, the information should include the classification of that asset in terms of risk and criticality.

Vulnerability Remediation

The NCSA Security Office group will work to incorporate the context of the finding by noting the classification of the asset and the severity of the vulnerability. Additionally, other factors may be considered such as the role of the vulnerable asset within NCSA. These factors will be used to ultimately determine the actual severity of the vulnerability.

The severity of the vulnerability will determine the required time for remediation. Vulnerabilities classified as “critical” need to be patched or remediated within 4 hours. These are vulnerabilities with the potential to have a severe impact on the NCSA. Vulnerabilities classified as “high” need to be patched or remediated within 24 hours. There are vulnerabilities with the potential to have significant impact on the NCSA. For lower vulnerability classifications: patching should occur within a planned maintenance cycle or a separate plan is made to patch or remediate the vulnerability within a reasonable timeframe.

In some rare cases, the vulnerability cannot be patched and remediation may not be adequate. An exception must be filed with the NCSA Security Office. The exception may generate significant risk and may need to be reported to NCSA Management for acceptance.

ACHE Vulnerability Remediation

The Advanced Computational Healthcare Enclave (ACHE) has a separate policy for vulnerability remediation stated below.

Standard Updates

Standard patches are performed during regular scheduled outages which occur at least twice a year and include basic OS updates (including security patches) and other updates from vendors. A full vulnerability scan is performed again after any planned maintenance (PM).

These quarterly PMs are generally done during weekends and off hours with prep work to minimize customer downtime. However, they may 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 an 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.

References

Understanding Severities in the SECURITY JIRA Queue https://wiki.ncsa.illinois.edu/display/SecOps/Understanding+Severities+in+the+SECURITY+JIRA+Queue