XES Vulnerability Resolution Procedures

Purpose

A critical part of maintaining XSEDE’s reputation and availability of services is to stay on top of the maintenance of the XSEDE Enterprise Services (XES). Most XES are managed by the SysOps team and hosted at the infrastructure providers funded by University of Illinois. Currently these are NICS, NCSA, PSC, and TACC. The purpose of this document is to explain the different responsibilities and roles as it relates to vulnerability management of these services and to describe the process, which spans SysOps and SecOps, a.k.a. Cybersecurity.

Roles and Responsibilities

In the vulnerability resolution process, SysOps, SecOps, local infrastructure provider staff, and system/service operators are all involved.

SysOps

XSEDE SysOps is responsible for maintaining and patching the XES, and the SysOps L3 manager maintains a list of responsible system operators. This L3 keeps the list up to date, assigns maintenance tasks (e.g., patching), and ensures they are completed.

SecOps

XSEDE SecOps is responsible for scanning these services, interpreting and prioritizing remediation, and reviewing residual risk when patches are purposefully delayed or left unpatched.

XES Infrastructure Providers and Operators

XSEDE infrastructure providers may provide hosting and system administration, or just hosting. Those infrastructure providers hosting XES are expected to provide a reliable platform with backup service, basic health monitoring and follow the XES Baseline Security Standard. System/service operators may be at the hosting infrastructure provider or elsewhere. These are the people responsible for the system administration and maintenance of the service. They must be responsive to SecOps and SysOps and follow the XSEDE Enterprise Services Baseline Security Standard. If they change roles and can no longer be the service operator, they must inform the SysOps L3 immediately.

Procedure

The following workflow is enforced by JIRA workflows and tracked in the SysOps/SecOps Kan Ban. This board guides the collaborative activities between SysOps and SecOps and drives the weekly coordination meetings between the L3 managers.

1. A Qualys scan is run regularly. As new findings are discovered, a SecOps team member creates tickets per issue for each service with an explanation of the vulnerabilities that need to be addressed and the software that should be updated or verified as up-to-date. This ticket is then moved from the backlog to the Accepted state, where it is assigned to the SysOps L3.
2. The SysOps L3 reviews the ticket and assigns it to the appropriate system operator, moving the ticket to the In Progress state.
3. Upon receipt of the ticket the service operator will ask for clarification and help from either the reporter or their site's representative on the XSEDE Security Working Group. There may be false positives or reasons not to patch that need to be discussed, but a plan of action should be recorded in the comments.
4. When the system operator has completed the work or suggested an alternative plan, it is marked for review. This assigns the ticket back to the original reporter for review. If a patch is going to be delayed more than two weeks, a comment should be added and it can be placed in the stalled state.
5. The reporter verifies that the issue has been addressed or mitigated appropriately, and then it moves to the Done state.
6. SysOps/SecOps L3's review and release issues at their regular meeting.