# XSEDE Enterprise Services

# Baseline Security Standard

*June 22, 2017*

Version 1.4

# Table of Contents

## A. Document History

| Relevant Sections | Version | Date | Changes | Author |
|---|---|---|---|---|
| Entire Document | 1.1 | 10/3/2013 | Baseline | A. Slagell |
| Entire Document | 1.2 | 1/20/2017 | Review of entire doc | V.Hazlewood<br>A. Slagell<br>J. Marsteller |
| Entire Document | 1.3 | 2/8/2017 | Review of entire doc | S. Sakai |
| Entire Document | 1.4 | 5/2/2017 | Accepted all changes and addressed comments | V. Hazlewood |
| Entire Document | 1.4 | 6/22/2017 | Addressed all the additional written comments/updates. Accepted by security team. See security team meeting minutes | V.Hazlewood<br>A. Slagell<br>J. Marsteller |

## B. Document Scope

Providers of XSEDE enterprise services shall follow this security baseline document developed and maintained by the XSEDE Security Working Group (XSWoG) and approved by XSEDE Operations management. Because of the natural trust relationships between major XSEDE resources and the interdependence of them, security vulnerabilities affect far more than a single service provider or XSEDE funded infrastructure provider. Therefore, this document sets forth minimum security standards for providers of XSEDE enterprise services (XES) whose compromise could have a direct impact upon XSEDE.

# C. XSEDE Enterprise Services Security Standards

## C.1. Introduction

Providers of XSEDE Enterprise Services (XES) shall follow this security baseline document developed and maintained by the XSEDE Security Working Group (XSWoG) and approved by XSEDE management. Because of the natural trust relationships between major XSEDE resources and the interdependence of them, security vulnerabilities affect far more than a single service provider or XSEDE funded infrastructure provider. Therefore, this document sets forth minimum security standards for providers of XES whose compromise could have a direct impact upon XSEDE.

## C.2. Definitions

**XSEDE Enterprise Services (XES):** These are XSEDE services, usually supported by an XSEDE funded infrastructure or cloud provider, which XSEDE users depend upon either directly or indirectly and whose integrity and availability affect more than a single service or infrastructure provider. While many of these services are exclusive to XSEDE (e.g, XDCDB, AMIE, and the XSEDE Kerberos realm) some serve other customers as well, such as, GlobusOnline. The XSEDE Operations Systems Operational Support (SysOps) group maintains the official list of XES.

## C.3. Security Standards

Items in this section are standards that establish a minimum baseline, i.e., part of the expectations for each enterprise service provided. Application for and approval of any exceptions to these standards must be sent to and approved by the XSEDE Director of Operations.

### C.3.1. Vulnerability Management

Some security incidents target existing vulnerabilities that have long since had remedies available. One of the most effective activities to reduce exposure and prevent incidents is to maintain up-to-date and properly patched software. This is true both for users at home, and those running entire data centers.

XES providers will:

- Maintain software patches such that they are up-to-date against *exploitable* vulnerabilities (for which there is a remedy) considered a *significant threat* to XSEDE.
- Be able to identify systems vulnerable to a particular exploit (whether there is a patch or not), and report back plans for risk mitigation
- Permit XSEDE to scan the XES resource using XSEDE's QualysGuard scanner for non-authenticated scans. Newly discovered vulnerabilities will be discussed on the regular XSWoG calls.

- XSEDE will not perform web application vulnerability scanning of an XES resource without a coordinated outage window due to the high potential for collateral damage.
- XSEDE XES providers may perform their own vulnerability scans, but such scans must not be in lieu of vulnerability scanning performed by XSEDE.

### C.3.2. Configuration Management

To ensure that services stay true to baselines, to provide for consistent replicas, and to be able to easily back out changes, XES need proper configuration management tools and change control process.

Therefore, XES providers must:

- Implement a practice that automatically restores configuration approved by XSWoG in the event of improper or unauthorized modification to the host's configuration.
- Implement a practice that will return a freshly-installed host to its XSWoG-approved configuration without manual reconfiguration.
- Follow and provide an acceptable change control process to the XSWoG for approval.

Note: A configuration management tool such as Puppet, cfEngine, or Ansible may be used to satisfy these requirements, however the use of a configuration management tool is not sufficient -- its application must provide the aforementioned capabilities.

### C.3.3. Authentication & Authorization

It is critical to control access to XSEDE resources, especially in cases of privileged access. It is equally important to accurately record who has access to systems and that they are not exceeding their authority. XES providers will:

- Use strong, i.e., at least two-factor authentication (2FA), authentication for administrative interfaces, accounts or privilege escalation where at all possible (see exception clause in C.3 above). This could be directly on a system or through use of a choke point such as a bastion host or VPN.
- Eliminate the use of ad-hoc accounts and passwords where possible (see exception clause in C.3 above).
- Prohibit the use of session-management applications (e.g. screen, vnc, remote desktop) in a manner that exposes an authenticated session to a user authenticated by a grade of authentication lower than that which was used to authenticate the session.
- Record audit logs of all authentication attempts, including privilege escalations.

- Maintain and audit the list of admins and privileged users to avoid authorization creep and to remove access when XSEDE staff or XSEDE infrastructure provider staff leave the project or roles change.

## C.3.4. Audit Logging

It is critical to maintain the integrity of system and network logs in order to investigate security incidents. XES providers will:

- Collect and maintain system and application logs (syslog) for at least one year and verify logging at least monthly if there is no continuous monitoring.
- Send all system and application logs for all systems running XES to the XSEDE syslog service.
- Maintain network time protocol on all servers running XES to maintain consistent timestamps across XES.

## C.3.5. Network Monitoring

System and authentication logs are very important but often not sufficient to investigate all anomalies and/or security incidents. Equally important are networks logs. While XES providers are not necessarily expected to run a full Intrusion Detection/Prevention System, which can be very costly, they do need to maintain NetFlow level logs and statistics at their borders. A service provider is expected to be able to answer if they have seen activity from specific IP addresses within a particular range of time. XES providers will:

- Maintain NetFlow or equivalent logs of source and destination IP addresses to or from XES servers
- Restrict connections to XES with appropriate host or network based firewalls when requested.

## C.3.6. Firewalls

A firewall capability implemented either with a firewall appliance or equivalent host-based firewall rules (e.g. iptables) must implement a deny-all allow by exception policy of IP and service access.

## C.3.7. Auditing

As configuration changes can accumulate over time, systems and services can drift from baselines. Therefore, it is expected that service providers audit themselves for compliance with this baseline at least annually and to report on the results. Critical XES will be audited regularly by the XSEDE security operations, and XES providers shall participate in these investigations and audits.

### C.3.8. Physical Access

XSEDE systems and services are not to be placed in public or unrestricted areas. They must be secured in a facility that has a way to audit who has access to rooms with these systems and preferably audit logs to confirm who has had access at a given time. If the latter is not possible, they need to physically restrict access to racks with XSEDE servers to a minimal list of employees. If outsourcing hosting to external providers such as Amazon, they must require that their external service provider has physical controls no lower than their own.

### C.3.9. XSEDE Security Working Group Access

Security is never a goal, but an ephemeral state that must be maintained in a dynamic environment. In order for XSEDE to identify situations that may require adjustment from their previously-approved configuration, or configurations that have deviated from their previously-approved configuration, XSEDE's Security Working Group requires some minimal level of access to every XES resource.

Hosts:

The XES provider shall create individual system accounts for XSWoG staff that permit accessing the resource via SSH pubkey or 2FA authentication.  These accounts must have sufficient privileges to enable configuration auditing, incident response, and security posture evaluation. XSWoG staff agree to manage their private key in a secure manner, resistant to offline dictionary attacks. XSWoG staff also agree to avoid making configuration changes to the system unless explicitly coordinated between the XES provider and XSEDE CISO.  The preferred method of change request by the security team is via the XSEDE ticket system to the XES system administrator.

Services:

The XES provider shall provide read-only access to XSWoG staff for the purpose of auditing configuration, incident response, and security posture evaluation.  Due to the varied nature of application services, these services and the level of access will be specified in an appendix to this document.  Where possible the security team member needing access to XES systems will be from the XES funded organization.