XSEDE Security Playbook

March 31, 2016

Version 1.1

Table of Contents

A. Document History

Relevant Sections	Version	Date	Changes	Author
Entire Document	1.0	7/25/2013	Baseline	A. Slagell
Entire Document	1.1	3/31/2016	Updated definition of the XSO and replaced Incident Response Team With Trust Group	A. Slagell

B. Document Scope

Incident response guidelines are provided for: responders at the Level 1 Service Provider (SP) where the initial incident occurs ("Initial Responder"), responders at any other Level 1 SPs ("Secondary Responders), XSEDE Help Desk or other persons who may receive the initial notice of an incident, and the XSEDE-wide Trust Group.

C. Document Body

C.1. Introduction

C.1.1. Scope

Incident response guidelines are provided for: responders at the Level 1 Service Provider (SP) where the initial incident occurs ("Initial Responder"), responders at any other Level 1 SPs ("Secondary Responders), XSEDE Help Desk or other persons who may receive the initial notice of an incident, and the XSEDE-wide Trust Group.

C.1.2. Definitions

- Incident: an event in which a compromise of a system or user account is suspected and being investigated. Incidents include actual compromises and investigations, which determine there was no compromise.
- Compromise: unauthorized access to a system ("root" compromise) or user account ("user" compromise). This includes activity by a user who may be authorized to do other things.
- Initial Responder: person handling the incident at site where complaint/problem originates.
- Secondary Responder: persons receiving notice of incident from the initial site.

C.1.3. Level 1 Service Providers are assumed to:

- have a current copy of the XSEDE Security Playbook (this document)
- be following the XSEDE Level 1 Baseline Security Standard
- have signed keys and passwords needed for confidential communications with other Level 1 SPs
- have a site-specific incident response plan

C.2. Incident Classification

In determining how to organize a response to an incident, its severity must be determined. This will affect the amount of collaboration needed and whether or not the incident investigation needs an XSEDE lead to organize the collaborative investigation.

The following classification for high, medium, and low is to be used in the ticket title and email subjects for any XSEDE security incident.

High: (XSEDE lead required)

The incident could lead to exploitation of the trust fabric, i.e. user and host identities, or the incident could lead to instability over all of XSEDE, or a denial-of-service is in progress against all replicas of a given XSEDE service.

Medium: (XSEDE lead only required if widespread)

The incident affects an instance of an XSEDE service, but XSEDE's stability is not at risk, or a denial-of-service affects one replica of a given XSEDE service, or a local attack compromised a privileged user account.

Low: (XSEDE lead is not needed)

A local attack comprised an individual user, non-privileged credentials, or a denial-of-service attack or compromise affects only local XSEDE resources.

C.3. Guidelines for Initial Responders

As soon as possible, notify the XSEDE Trust Group by sending an email to incident-report@xsede.org. If required, site-specific contact information is listed in XSEDE Security Contact List[1]. Provide whatever information is available (see below for types of information), so that secondary responders may check their sites as necessary. Designate a point of contact at your site that can coordinate communications with secondary responders. Notify sites of the earliest time you can be available for a conference call. XSEDE has a 24-hour emergency hotline available for incident response coordination that is known only to the Incident Trust Group and select Security personnel (see Appendix B).

Sensitive email sent to the Incidents list must be encrypted using PGP/GPG. Details can be obtained from the XSEDE Security Office (XSO). Email to individual Security/Incident Response personnel may be encrypted using their PGP keys. Keys are regularly exchanged and signed at annual XSEDE meetings and can also be obtained the XSO, whose members have signed them all.

The Security Working Group uses a secure site and instant messaging service for incident documentation and sharing. The secure wiki has a section for tracking incident information and SP responses. Incident details should be shared on the wiki for coordinating across the XSEDE SPs. The encrypted jabber service can be used for information sharing and response coordination in real time.

When sharing information, be sure to indicate clearly any information shared which should not be publicized. The secure Wiki Provide updates as information becomes available. If a compromise is confirmed, notify sites as soon as possible.

Expect to provide the following information as available and relevant:

- Hosts affected at your site; User accounts affected; and Source of compromise (remote hosts)

[1] https://ops-security.xsede.org/wiki/XSEDE_Security_Contact_List

- Nature of compromise (e.g. remote vulnerability, local vulnerability, etc.)
- Signatures of compromise (log messages, files installed/modified, etc.)
- Other XSEDE sites, which may have been touched by intruders
- Completed Compromised User Account Questionnaire in Appendix A .

When incident is resolved, send an incident report out to XSEDE sites following guidelines in Appendix A.

Notify the XSEDE Security Office (security-lead@xsede.org) in the event of any incident or compromise prior to disclosing such incident or compromise outside of local management. This ensures timely and accurate disclosure, as necessary, to the National Science Foundation.

C.4. Guidelines for Secondary Responders

Follow your own site procedures for handling security incidents.

Be aware of confidentiality requirements for information you will receive from other sites; do not re-share such information without their permission.

If an incident requires action by a secondary responder, it should be tracked on the secure wiki pertaining to the incident. It is important that all responses are documented and accounted on the secure wiki to minimize risk to the XSEDE project.

Notify other contacts of the soonest time you can be available for a conference call. The call number is included below in Appendix B.

After the incident is over, report out to XSEDE Level 1 SPs using guidelines shown in Appendix A below.

C.5. Guidelines for Help Desk

Follow the XSEDE Security Incident Flowchart in Appendix B.

Inform your site security contact as soon as possible. Be aware that an intruder may be monitoring network traffic and e-mail; a phone call is advisable. Do not forward incident information to other parties; let the site security contact do that.

C.6. Guidelines for Public Relations

Information about compromises, or information provided by sites other than your own is to be considered confidential and not to be disclosed without permission. Each site may follow its own disclosure guidelines or requirements about compromises for their own information but should not disclose information about compromises at any other XSEDE SP. At no time should anyone com-

ment on XSEDE security related issues to outside parties, only the XSEDE Security Office and XSEDE Project Office.

D. Appendix A — incident Reporting Guidelines

D.1. Compromised Account Questionnaire

To be conducted by a member of User Services/Operations and a member of the security working group.

- Do you use the password of the account at other XSEDE sites or other general accounts (Google, Amazon, Facebook, Twitter, etc.)?
- What was the time of your last known login? Where was it from?
- From what locations do you usually login (hostnames/IP)?
- Which SPs/XSEDE resources have you used recently?
- What locations (hosts) can we expect to you to login from?
- Can accounts at other XSEDE sites be closed down, or do you expect to use them in the future? If so, which sites are needed: (PSC, SDSC, NCSA, Purdue, Indiana, NICS, TACC, etc.)
- Are passwords needed on all the sites, or are you using grid certificates or ssh keys? Since the account was compromised, are there any special concerns on the data exposed? Any PII or confidential data? Any private keys?
- Do you have any idea how someone may have gotten your account credentials?
- What machines may possibly be compromised (your desktop or some other machine you used)?
- Have you been contacted by any other sites related to this compromised account?
- If possible, please provide contact information for you local Security team.

D.2. Site Incident Report

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.

- How much time (in person-hours) did staff at your site spend dealing with the incident?
- How were you notified?
- What steps did you take to investigate if there was a compromised account or system at your site?

- What did you determine?
- If there was a compromise:
    - What damage was done?
    - What steps did you take to respond/recover?

E. Appendix B — XSEDE Security Communications

E.1. XSEDE Emergency Hotline

This number is to be used only for conference calls for XSEDE inter-site incident response. This number is *not* to be used for weekly conference calls or other purposes.

The number does not require prior scheduling for use; it is available 7/24.

- Toll Free Dial In Number: 1-866-295-5950
- Int'l Access/Caller Paid Dial In Number: 1-978-964-0031
- HOST CODE: (Ask your site security lead)
- PARTICIPANT CODE: (Ask your site security lead)

E.2. XSEDE Incident Response Mailing Lists

E.2.1. Security Working Group (ops-security@xsede.org)

This list is used for non-incident related discussions with the whole XSEDE Security Working Group, of which the XSEDE Trust Group largely overlaps. The XSEDE Security Working Group (XSWoG) Charter can be found on the User Portal[2].

E.2.2. Incident (incident-report@xsede.org)

This list is used to communicate critical security event information that requires immediate attention of the XSEDE Trust Group. Because mail sent to this list may trigger emergency notification and escalation action, it should only be used for security emergencies that directly affect the XSEDE project. Subscription to this list is determined by the Incident Response contact per site as detailed in the XSEDE Security Contact List[3].

E.2.3. Incident Discuss (incident-discuss@xsede.org)

The primary purpose for this list is to announce Incident Response meeting details and share "non-critical" Incident Response information with the XSEDE Trust Group. Security Working Group members may send requests to the XSEDE Security Office to be added to the incidents-discuss list.

E.3. XSEDE Incident Response Secure Wiki

The Security Working Group uses a secure site for incident documentation. Information about this site is provided to incident handlers from the Security Working Group as needed. This is separate

[2] https://www.xsede.org/documents/10157/247425/XSEDE+Security+Working+Group+Charter.docx

[3] https://ops-security.xsede.org/wiki/XSEDE_Security_Contact_List

from the general XSEDE staff wiki, which has more granular access control and can be found at https://ops-security.xsede.org.

E.4. Secure Jabber Server

You can contact the XSEDE Security Office if you would like access to the encrypted, dedicated Jabber IM service for XSEDE Trust Group. Configuration information is found on the XSEDE Incident Response Wiki described above.

F. Appendix C: XSEDE Security Incident Flowchart