OSG Incident Response Policies and Procedures

v1.0
Last updated on 12/1/2019

Authors: Zalak Shah
Information Security Officer: Mike Stanfield

Table of Contents

1 Introduction and Scope

This document covers policies and procedures for handling computer security incidents impacting infrastructure owned and operated by the OSG project, or software developed, maintained, or distributed by OSG. This includes publicly accessible OSG services, supporting infrastructure, and infrastructure used by OSG staff essential to the OSG mission (e.g. systems supporting OSG development and personal workstations of OSG staff with administrative access).

This document does NOT cover incidents at resource provider's sites and virtual organizations (VOs). While OSG Security Team will make ourselves available to the extent possible to help with such incidents, they are outside of our scope of control and responsibility.

An information security **incident** (henceforth an "incident") is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of information or security policies, security procedures, or acceptable use policies. Discovery of a vulnerability in one or more pieces of software or dependencies of the OSG services could also cause an incident. An incident may involve malicious entities, accidents, or any state that poses risk.

Policies of institutions which house the staff and infrastructure comprising the OSG project and facility (i.e.University of California - San Diego, University of Wisconsin-Madison, University of Nebraska - Lincoln, Indiana University, University of Chicago) could potentially be found to be in conflict with this policy under unforeseen circumstances. In that event, staff or infrastructure are bound by the policies of their housing institution. No such conflict is known and if any such conflict is discovered, it must be brought to the attention of the OSG Information Security Officer (ISO) immediately.

2 Goals of OSG Incident Response

Any process should have prioritized goals to guide tactical and time-critical decisions. For OSG incident response, the goals are, in decreasing priority:

1. Minimize negative impacts from an incident in terms of:
    a. loss of integrity of OSG services or data entrusted to those services
    b. negative impact to resource providers' systems as a result of their OSG participation
    c. negative impact cause to consumers of OSG-developed, maintained, or distributed software
    d. damage to OSG reputation due to actual security issues or perceived risk / lack of trust.
2. Protect the confidentiality of non-public information entrusted to OSG systems and services.
3. Keep OSG management and stakeholders informed.
4. Collect information needed to understand the specific impact the incident had on OSG and prevent future incidents.
5. Maintain the operational availability of OSG services to its user community.
6. Collect evidence needed for identifying or prosecuting perpetrators.

These priorities may be adjusted by the OSG ISO for a particular incident. For example, multiple incidents perceived to be caused by the same perpetrator may increase the priority of identifying that perpetrator and collecting evidence, as removing a persistent attacker supports higher priority objectives.

3 Roles, Responsibilities, and Authority

The following list includes primary entities involved in incident response and their general responsibilities. This is intended to offer more detail specific to incident response, and does not override anything written in the MISPP. Additional, specific responsibilities are addressed in Sections 5 and 6.

- OSG Incident Response Team ("IR Team")
  - An incident-specific, ad-hoc team formed to handle an incident.
  - Will often include members of Security, Software, Operations and Release teams, but actual composition will vary depending on the nature of each incident.
- OSG Incident Response Lead
  - Designated Security team member assigned by ISO.
  - Responsibilities:
    - Set incident classification.
    - Sends reports of incident progress to the ISO regularly
    - Ensure the relevant policies and procedures in this document and elsewhere are followed
    - Assemble and direct IR team
    - Ensure that a complete and correct record of the incident is maintained
    - Ensure that a complete and correct IR report is written
  - Authorities:
    - Act in place of the ISO making cybersecurity risk decisions during an incident if needed when the ISO[1] is unavailable.
    - Authorize the suspension or removal of any OSG resource, user, service, job, VO, etc. until the incident has been resolved and related issues remediated.
    - Determine what remediations are appropriate to resolve an incident, and oversee the process of incident response.
    - Enlist OSG staff to assist with incident response or join the Incident Response team, ideally in coordination with their management.
- OSG Service Owners:
  - Refer to the OSG Service Catalog for Point of Contact for various OSG services.
  - Responsibilities:
    - Leads interactions with their campus security and IT staff[2].
    - Assists the IR team as needed in responding to an incident, for example by retrieving logs from affected systems, or making prescribed changes to remediate vulnerabilities.
  - Authorities:
    - Disconnect the OSG service from the network, ideally in consultation with the OSG ISO and OSG Management.
    - Suspend OSG users and similar entities.
- Resource Provider administrator, VO administrator or security point of contact:
  - Responsibilities

[1] For statements such as this, there is an implied "and backups" for the role under discussion, hence the chain of authority is ISO, backup ISO, IR Lead.

[2] The OSG Service Owner owns this responsibility since they are physically located at a different institution where the ISO is not.

        - Work with relevant site's local security team during an incident, as appropriate.
        - Inform the OSG Security team of any incident locally which may impact OSG or the site's participation in OSG.
        - Coordinate with the OSG IR team in the case of any incident that impacts multiple sites, services, or other parties across OSG.
        - Remove the resource center or VO from OSG if it may be harming OSG or OSG users/resources as a result of an ongoing security incident.
    - Authorities
        - Request to the OSG ISO or IR Lead to approve the reconnection of the resource center or VO to OSG after issues related to a security incident have been remediated.
- OSG ISO (Stanfield, IU):
    - Backups, in order of preference:
        - Zalak Shah, IU
        - Josh Drake, IU
        - Any other active member of the OSG Security Team
    - Responsibilities:
        - Ensures regular communication with OSG Management and stakeholders as needed during an incident.
        - Ensures appropriate communication with OSG users regarding incidents.
        - Ensures appropriate communication with other institutions' Security Offices if needed.
    - Authorities:
        - Declares a security incident, when deemed necessary, and names an Incident Response Lead for that incident.
-
- OSG Security Team (Shah, Stanfield, Drake, Krenshaw IU, Teheran FNL):
    - Responsibilities:
        - Help as requested by the IR Lead during an incident.
        - Perform post-mortem analysis of incident in conjunction with the IR team and other relevant parties.
        - Maintain readiness for incidents.
        - Own the follow-through on issues discovered during incidents and security exercises.

4 Incident Response Stages

The OSG's incident response strategy is described in this section based on the anticipated stages of an incident.

4.1 Preparation

The OSG Security team, service owners, Operations and Software teams will maintain the following on an ongoing basis to be prepared for any incident:

- The Security and other OSG teams will have appropriate information to allow for secure communications during an incident (e.g. phone numbers, GPG keys).
- The security team will work with server owners to establish centralized (per site) system logging

and an appropriate level of network logging, to allow for analysis and with a retention window of at least 90 days, as resources become available for these changes.
- An infrastructure map detailing all OSG computers and logical network layout will be maintained and updated at least every 30 days.
- A list of IP addresses and their associated network hosts will be maintained and updated at least every 30 days.
- The OSG Security team, with the help of the service owners, will maintain an up-to-date inventory of all the software packages and dependencies for each individual OSG service.
- The OSG Security team will monitor notifications/announcements regarding the vulnerabilities and security patches on a regular basis and will check whether any of the vulnerabilities could potentially affect the OSG service(s) or the users based on an existing inventory.
- The OSG Security team's web page under GitHub https://opensciencegrid.org/security/ will have directions for OSG users and other outside parties about how they can report a security incident to the OSG. To contact the OSG Security team regarding a suspected incident please email security@opensciencegrid.org - you may encrypt your email for privacy using GPG (Key id#7FD42669, fingerprint 6E5F 4DD8 7ABC 9F68 A49B F3CA 15E3 B3AD 7FD4 2669).
- The Security team will regularly audit the above items to ensure they are in place and lead a monthly security exercise to ensure preparedness and increase the maturity of operational security at OSG.

4.2 Incident Initialization

Potential or known incidents may be reported by the OSG staff, OSG users, or third parties such as incident reporting or coordination organizations.

Notification from the OSG staff, and reports from OSG users and third parties should go directly to the OSG Security team.

ACTION by OSG team Member who first becomes aware of the potential incident: The team member should:

1. Attempt to contact the ISO (Mike Stanfield).
2. Failing that, attempt to contact a Backup ISO from the list in section 3 of this document. The Backup ISO, when contacted, will act in place of the ISO for the purpose of incident-related authority and responsibilities named in section 3 above.
3. If no ISO or backup ISO is reachable (rare) contact any member of the OSG Executive Team for further instructions.

ACTION by ISO: The ISO will make the determination of whether an occurrence is an incident.

ACTION by ISO: If determined to be an incident, the ISO will assign it an identifier based on a template of <year>-<month>-<day>_<sequential number>, e.g. "2019-03-18_001"[3].

ACTION by ISO: When an occurrence is identified as an incident, the ISO will set an initial priority of either high or normal:

- **High priority** means that the OSG Security team members are expected to handle any request

[3] For an exercise, append "_EXERCISE" to the name, e.g. "2019-03-18_001_EXERCISE"

related to the incident in preference to all other work.
- **Normal priority** means that the OSG Security team members are expected to prioritize incident handling using their judgement.

Setting priorities is a subjective process, with the level of certainty the incident represents a compromise of the OSG and the impact of the compromise playing significant roles. Prioritization is expected to track classification as defined in Section 5 but will be set before classification has been determined.

4.3 Formation of Incident Response Team

ACTION by ISO: The ISO will designate and contact an Incident Response Lead.

ACTION by IR Lead: The IR Lead will determine what personnel are needed on the IR team and contact those individuals.

ACTION by IR Lead: The Incident Response lead should communicate the initiation of an incident by sending an email to staff@opensciencegrid.org with the priority and make up of the Incident Response team in the body. As with any email about the incident, the incident identifier will be used in the subject of any email message. Do not describe the exact nature of an incident here, as this email traffic is widely distributed in the clear.

ACTION by IR Lead: The IR Lead will create a JIRA issue in the Security project to store data regarding the incident[4]. Set the Security Level to "Security team" so that the issue will only be viewable by the OSG Security team.

4.4 Analysis and Containment

Guided by the Goals of OSG Incident Response, the Incident Response team will initially work to contain the incident, minimizing its impact to the OSG, and determine its nature. During this phase, changes should be minimized to what is necessary to prevent further damage in order to preserve evidence.

ACTION by the IR Lead, IR Team: The Incident Response team will conduct the investigation, with other OSG staff assisting as needed.

During this phase, the IR Lead may change the prioritization of the incident or the membership of the Incident Response team based on an evolving understanding of the incident.

During this phase, it is important not to modify or alter any logs or configuration unless it is urgent and critical to maintaining the confidentiality or integrity of other data. This is to maintain useful forensics. If alteration is necessary, careful notes (or screenshots, etc.) must be taken so that the original state prior to the change can be reconstructed. Notice of the alteration must be communicated to the Security team and IR Lead immediately.

ACTION by IR Lead: The IR Lead will keep the ISO informed of any major developments and discoveries, making at least twice a day updates.

ACTION by IR Lead: The IR Lead will keep OSG User Support (user-support@opensciencegrid.org) informed of any user-visible service impacts of the incident.

[4] https://opensciencegrid.atlassian.net/projects/SECURITY/issues

The incident identifier will be used in the subject of any email message related to the incident.

4.5 Eradication and Recovery

During this phase, the Security team will make a recommendation (suggesting, for example, a code or configuration change) to the Software team and or Service owner on how to manage the vulnerability, based on the relevant vulnerability report or an analysis of flaws in OSG-maintained code. This recommendation, especially when addressing flaws in OSG code, should be made in careful consultation with the relevant service or software owner.

ACTION by IR Lead: The IR Lead will continue to keep the ISO informed of any major developments, making at least twice a day updates.

ACTION by IR Lead: The IR lead will continue to keep OSG User Support informed of any user-visible service impacts of the incident.

ACTION by IR Team: If necessary, a member of the IR team in consultation with the other IR team members will send an update to the user community about when they should expect a security release and what they can do to mitigate the issue in the meantime.

The incident identifier will be used in the subject of any email message related to the incident.

4.6 Incident Closure and Documentation

ACTION by IR Lead: After consulting with the ISO, the IR Lead will mark the JIRA issue for the incident as Resolved and communicate the incident conclusion by sending an email to staff@opensciencegrid.org.

ACTION by IR Lead: The IR Lead will document the incident, including its classification as described in Section 5. The documentation should use the OSG IR Template.

4.7 Post-Mortem and Remedial Action

ACTION by ISO: The ISO will note any suspended accounts, projects, etc. from the incident report and determine a long-term disposition for those.

ACTION by ISO: The ISO or delegate will lead a post-mortem that consists of determining what remedial action should be taken to minimize the chance of the incident repeating and work with OSG Management to implement such remediation.

5 Incident Handling Procedures

5.1 Incident Classification

OSG incidents are classified based on their perceived impact. Classification may not be known at the start of an incident due to lack of information and may change as understanding of the incident improves. This classification guides responses as described elsewhere in this document. These classifications are based on those in [NIST 800-61] Section 3.2.6.

N.B. Normally, an incident classified as “High” here is high priority per section 4.2 above, and all others are considered medium priority. However, some incidents may be up-classed to high at the discretion of the IR Lead if they present a contagious or potentially contagious problem: e.g. an APT targeting multiple

OSG, HTC, or HEP targets, self-propagating malware, or a moderate impact software vulnerability in a near-ubiquitous dependency that will be difficult to remediate or work around due to its pervasiveness.

Incident classifications are:

- High: An incident is considered High if it involves:
    - Compromise of confidentiality or integrity of PII[5].
    - Compromise of confidentiality or integrity of a password database.
    - Compromise of confidentiality or integrity of software vulnerability information.
    - Attention by media outlets or other public dissemination (e.g. via an Internet social media site).
    - Major disruption to the OSG's ability to provide service to the user community.
    - A successful compromise is believed to have been ongoing for more than a week.
    - An incident is believed to have possible financial consequences.
    - An incident is believed to involve an insider threat.
    - A high-severity vulnerability, including:
        - vulnerabilities that allow an unauthenticated attacker to execute arbitrary code or escalate privileges.
        - vulnerabilities that allow an attacker to access or exfiltrate data that is not theirs from the core system.
- Medium: An incident is considered Medium if it involves:
    - Disruption to the OSG's ability to provide service to multiple users for an extended time (more than 10 minutes).
    - Compromise of multiple users' accounts by the same party.
    - Any compromise that appears to specifically target OSG personnel.
    - A medium-severity vulnerability-
        - allows a local user to gain privileges.
        - allows an authenticated remote user to execute arbitrary code somewhere other than their host belonging to their jobs.
        - that lowers the difficulty of denial of service attempts.
- Low: An incident is considered Low if it involves:
    - Disruption to a single user's ability to use the OSG (e.g. a compromised password that results in temporarily disabling their account).
    - A short-term (less than 10 minutes) disruption in OSG's availability due to a denial of service attack.
    - A long-term disruption to non-critical services or degradation of critical services.
    - Attempted but unsuccessful attempt to compromise the OSG service in some way that appears to target the OSG specifically and is not normal untargeted Internet "background noise."
    - A low-severity vulnerability-
        - one that has a cosmetic-only or has an inconvenience impact rather than a compromise of confidentiality, integrity, or availability.
    - Vulnerabilities that have high or medium impact but are especially difficult to exploit.
- Undetermined: Impact of an incident is unknown.

[5] It is the belief of the Security team that the OSG does not hold Sensitive PII as of the date of publication of this document.

- Prioritization will be determined by classification level set by the ISO and IR Lead based on the available data.

5.2 Secure Communication During Incidents

During an incident investigation, members of the IR team may need to share sensitive information and discuss suspected vulnerabilities in the OSG. The following methods of communication of sensitive data are approved:

- OSG JIRA, using the Security Project
- S/MIME encrypted and signed email
- GPG-encrypted and signed email
  - It has been noted that GPG signatures are fragile and often do not validate for benign reasons. Staff should also validate a request using an alternate channel if they have any doubt as to the legitimacy of a message.
  - It has been noted that emails are not predictable in their delivery latency and cannot be relied on for timely communication.
- Phone (voice & secure message app Signal)
- In person
- IU Slashtmp (https://www.slashtmp.iu.edu/) - CRITICAL version
  - Transfers must be initiated by IU account holder

When communication of sensitive data using an approved method is not possible (e.g. not all management is familiar with the above methods), OSG personnel must exercise judgment regarding the method, content, and timing of related communications.

Integrity of communications is also important, particularly when instructions are sent or requests for sensitive data are made. Secure communications should be used for such circumstances.

5.3 Incident Handling After Normal Working Hours

OSG staff are not expected to work outside of normal working hours unless special arrangements have been made by the OSG management. Given that the integrity of OSG data[6] is more important than its availability, a reasonable response to an incident outside of normal working hours is to take the affected OSG service offline until the next business day. Taking the OSG service offline is done by contacting the Service owner.

5.4 Communication with User Support

OSG User Support is one of the interfaces to our user community. They might see reports from our users before the rest of the team and respond to those reports. Hence, it is valuable to keep them informed during an incident of factors that may impact our users so that (1) they can best communicate to users who may contact them and (2) alert the IR team if a user reports something that we are not aware of. User Support will forward the advisory or recommendation along with the security patches (if available) for known vulnerabilities to our user community. The IR Lead and/or ISO should keep them informed via email to user-support@opensciencegrid.org during the incident.

6 Interactions with Other Entities

[6] For example, source code and configuration data for OSG services

6.1 Law Enforcement

When and if an incident should be reported to law enforcement will be decided by the OSG ISO in consultation with OSG Management. All communications with Law Enforcement will be handled by the ISO and Executive Director, or at their direction.

6.2 Media and General Public

All media communication will be handled by the OSG Executive Director or their designee. Any OSG staff contacted by the media should refer them to the Executive Director unless authorized by the Executive Director to communicate with the media.

6.3 Incident Reporting/Coordination Organizations

The OSG ISO may decide to report any incident to incident reporting or coordination organizations (e.g. US CERT, REN-ISAC, EGI, WLCG). OSG staff should not do so without consultation with the OSG ISO.

6.4 Other institutions hosting OSG Services

The OSG Security team will communicate with other institutions hosting OSG services such as UW-Madison, University of Chicago, UCSD and UNL staff as needed during the incident.

6.5 OSG Users

OSG users should be kept informed as determined by the IR Lead.

OSG users are also encouraged to keep their Security and Admin contacts up to date.

6.6 Other Outside Parties

Other parties include owners of attacking addresses, other affected parties, software vendors, and other incident response teams. See section 2.3.4.4 of [NIST 800-61] for a discussion of these interactions. The IR Lead coordinates all such interactions.

8 Abbreviations and Acronyms

- APT: Advanced Persistent Threat, i.e. a skilled attacker persistently targeting something specific
- HEP: High-Energy Physics
- HTC: High-Throughput Computing
- ISO: Information Security Officer
- IDS: Intrusion Detection System
- IT: Information Technology
- OSG: Open Science Grid
- PII: Personally Identifiable Information
- UW: University of Wisconsin, Madison

9 Reference Documents

- [NIST 800-61] NIST Computer Security Incident Handling Guide. http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
- [CERT 2006] Action List for Developing a Computer Security Incident Response Team (CSIRT). http://www.cert.org/incident-management/csirt-development/action-list.cfm

10 Appendix: Procedure for Vulnerability Management

A vulnerability is a coding flaw, glitch or weakness that impacts OSG and/or OSG Services.

Preparation: The Security team monitors relevant vulnerability reports, announcements, and discussions on a regular basis. The Security team maintains an inventory of all the software, tools, and dependencies that have been installed on various OSG services. The Security team also keeps a contact list of important stakeholders ready and updated. We have published our PGP public key on OSG's website to enable outside parties to easily reach out with vulnerability reports.

OSG users are encouraged to report all the security issues, including software vulnerabilities, to the Security team at security@opensciencegrid.org.

Initial Report: Whenever the Security team receives a new vulnerability report, announcement, or an alert from OSG users, the Security team compares the name of the software/package to the inventory to check if we are running the affected software/package at the affected version. Upon examination, the Security team creates a private JIRA ticket indicating it is an incident with the sec-low/sec-med/sec-high/sec-critical label. The Security team uses the same JIRA ticket for all the internal discussions regarding the vulnerability to maintain confidentiality.

If the vulnerability was reported by a third party, the Security team will coordinate the tentative timeline with the reporter and will keep them updated if anything changes. The Security team will also ask them not to disclose the reported vulnerability and/or an exploit until we publish the fix for the vulnerability, and will discuss if and how the reporter would like their work to be credited.

Triage: The Security team will triage the vulnerability reports to determine whether the reported vulnerability is within scope for our action, by asking the following questions:

1. Does the reported vulnerability impact the security of OSG services, or currently-supported software developed/maintained by OSG?
2. Does the reported vulnerability impact the security of software distributed by OSG?
3. Does the reported vulnerability fail the first two tests above, but negatively impact the security of the OSG community in a significant way?

If the answer to either of the first two questions is 'yes' the security team will begin responding to the vulnerability. If the answer to the third question is 'yes', the security team may, but is not required to, make a best-effort attempt to notify the community about the implications of the issue. All other vulnerabilities are out of scope.

ACTION by the Security team: A member of the Security team will triage the vulnerability reports to determine their relevance and impact.

Analysis: For vulnerabilities deemed within scope, the Security team will assess the risk associated with the vulnerability in consultation with other OSG teams, software provider, and other appropriate parties.

Based on the assessment, risk will be addressed in one of the three ways, i.e. remediate, mitigate, or

accept.

1. Remediate: Apply a patch and resolve the vulnerability

   Vulnerability? -> develop a patch -> apply that patch -> TEST -> release a new version -> ask users to update to the new version

   The Security team also analyzes whether a reported vulnerability is worthy of a security release. The Security team makes that decision based on the severity, for example described in the report of Common Vulnerability Scoring System (CVSS).

   The Security team and other involved parties will work on a patch/fix in a private manner.

   - They will use a private ticketing system (JIRA) and include only a small group of developers to work on a private (non-published) git branch
   - Software Team (or other software owner) retains control of the software and handles the remediation process with support from the Security Team. It is important that software is *never* left in a state unfamiliar to its owners, e.g. by security team taking over and implementing a fix on their own.
   - Git commit messages do not include any vulnerability related information, they use something like “address issues outlined in ticket XXXX”

2. Mitigate: Find an alternative/temporary solution to minimize the impact or the likelihood

3. Accept: Accept the risk without remediation or mitigation

The Security team also prepares an advisory for the OSG users.

Disclosure: The Security team will coordinate a public release date with the downstream providers and important stakeholders. They will also make sure that critical infrastructure partners update their systems on the same day.

On a public release date, the Software team will merge the private (non-published) branch and will not provide any details about the exploit. The Security team will provide enough details about the vulnerability so that the OSG users could assess their risk and exposure but will not disclose any details on how to exploit the vulnerability. The Security team will restrict the JIRA ticket details for at least 30 days after a public release date and then make that ticket and the whole of the vulnerability details public.

The Security team may revise the public release date as needed, in consultation with the involved parties. After having all the necessary information about the vulnerability, the Security team will prepare a security announcement.

All the communications to and from the reporter and the communications with the OSG users will be done in a private manner.