Open Science Grid

Open Science Grid

Grid Security Incident Handling and Response Guide

Issue	Date	Comment
0.1	30 Aug 2004	Draft release to the Activity Group
0.2	7 Sept 2004	Draft release to the OSG Workshop, Sept 9-10
0.3	10 Nov 2004	Draft release to the OSG, Nov. 10
1.0	20 Nov 2004	Initial release of Incident Response Document

i. Document Development Milestones:

September 6, 2004: An abbreviated draft was presented to OSG and iVDGL committees for review and discussion during the Sept 9-10 OSG Workshop.

November, 2004: Progress in content development, especially aiming for harmonization with EGEE efforts, in preparation for the Second EGEE Conference, November 22-26, 2004.

Spring 2005: Guidelines developed and processes and services implemented as necessary for OSG.

ii. Credits:

This document was developed through the work of the OSG Security Incident Handling Activity Group*, including members Bob Cowles (SLAC), Mark Green (U Buffalo), Michael Helm (ESnet/LBNL), Doug Olson (LBNL), Doug Pearson (IU/REN-ISAC), Dane Skow (Fermilab), Tom Throwe (BNL), and Von Welch (NCSA); and with background developed through the prior works of Yuri Demchenko (University of Amsterdam).

iii. Contact:

Comments, questions, etc. may be referred through the OSG Security Incident Handling Activity Group chair, Doug Pearson <dodpears@indiana.edu>.

* OSG Security Incident Handling Activity Group http://www.opensciencegrid.org/activities/incident-response/index.html

1. Introduction

The cyberspace defined by Grids transcends organizational boundaries. Although the Grid doesn't create fundamentally new cyber security risks, it does serve to amplify some risks. The character of the security vulnerabilities and risks presented by Grid cyberspace provides a rationale for coordination among the Grid participants for cyber security incident response.

2. Purpose

This document presents the required and recommended support for security incident handling and response for Grids. It describes policy elements necessary for coordinated incident response (MUST) and policy elements constituting "good citizenship" for Grid participants (SHOULD) whether they are user organizations, sites, or resource/service providers.

Ultimately the purpose behind the development of this document is to reduce the incidence, severity, and exposure of Grids to cyber security incidents and to increase confidence of cyber security personnel that grids may be implemented without unduly increasing the risks to resources for which they are responsible. An *incident* is any real or suspected event that poses a real or potential threat the integrity of services, resources, infrastructure, or identities.

3. Policies

3.1. Reporting and Responding to Grid Incidents

Grid participants MUST report incidents that have known or potential impact or relationship to Grid resources, services, or identities.

Grid participants MUST respond to incidents involving locally managed or operated resources, services, or identities.

3.2. Handling of Sensitive Data

3.2.1. Incident information

Detailed and specific incident information is shared outside of a local site only within the *ad hoc* group of individuals actively working on the incident. These individuals MUST commit to using appropriate safeguards to protect sensitive or privacy-related information included n the incident information even after they are no longer actively working on the incident.

General incident information is shared with the grid security contacts and includes information such as identification of hosts, institutions, and individuals involved in the incident. Additional incident details from a site may be shared consistent with that local site's policies and procedures.

Nothing in these policies is meant to restrict the flow of information from a site to CERTs or other organizations to which the site is required to report incidents.

Public disclosure of information regarding security events SHOULD be handled through the site Public Relations contacts and SHOULD NOT contain more than summary information except for incident details related to specifics at the site.

3.2.2. Preservation of supporting data and evidence collection

All supporting data for an incident MUST be treated consistent with the site's rules for maintaining and storing such materials in non-grid incidents. Collection and coordination of evidence between sites is expected to be handled by the appropriate law enforcement agencies.

4. Organizational Structure

4.1. Security Contacts

Grid participants (user organization, service, or resource) MUST provide grid security contact information. Whenever possible, the information supplied SHOULD include monitored email lists in addition to, but not replacing, detailed contact information for specific individuals.

The grid security contact information is maintained by appropriate grid operations centers. The list contents are circulated to the email list when it is updated or at least once a month as to help promote currency of the information.

4.2. Response technical experts and response team leader

The individuals on the email list of grid security contacts comprise a body of technical experts to provide advice. Depending upon the severity, complexity, duration, and scope of an incident, adequate response may require the designation of a team leader who coordinates response process, maintains the flow of information regarding incident status, and coordinates with the grid operations center for supporting services.

4.3. Grid operations center

The grid operations center maintains the grid security contact email lists, and an archived mailing list server. It also monitors publicly accessible email addresses for reports of security incidents or abuse.

5. Supporting Resources

5.1. Mailing Lists

The grid operations center maintains two mailing lists to support incident reporting, analysis, and response. While it may be desirable for the mailing lists to support encrypted and signed communications, the initial requirement is merely to not interfere with signed email (PGP or S/MIME protocols).

In the following, xxx.yyy is replaced with the respective Grid, e.g. opensciencegrid.org.

INCIDENT-REPORT-L@xxx.yyy is a closed list comprising the grid security contacts for all grid participants and the grid operations center. Posting is restricted to list members. The list is intended solely for initial incident reporting, not for incident discussion. All email to this list is echoed onto the discussion list and replies are configured to be sent to the discussion list to keep traffic at a minimum.

INCIDENT-DISCUSS-L@xxx.yyy is a closed list comprising the same members as INCIDENT-REPORT-L. The list is intended for discussion of reported incidents.

The differentiation between INCIDENT-REPORT-L and INCIDENT-DISCUSS-L is to allow automated alerting mechanisms to be driven by the arrival of new messages in INCIDENT-REPORT-L.

Grid security contacts utilize INCIDENT-REPORT-L and INCIDENT-DISCUSS-L to communicate regarding security incident handling and response. Communications on both lists SHOULD be signed.

The standard email addresses *abuse@xxx.yyy* and *security@xxx.yyy* are received by the grid operations center, filtered for SPAM or other off-topic email and forwarded to the reporting or discussion list as appropriate. The grid operations center provides acknowledgements (possibly automated) for incidents reported through these external addresses.

6. Process

The processes for incident handling and response are:

1. Discovery and reporting
2. Initial analysis and classification
3. Containment
4. Notification and escalation
5. Analysis and response
6. Post-incident analysis

6.1. Discovery and Reporting

Incidents will be discovered through a variety of means including users, system administrators, engineers, and peers; operations center monitoring of infrastructure, services, and resources; and through monitoring of intelligence channels.

When an incident is discovered that relates to grid resources, services or identity, it MUST be reported to the local institution incident handling process AND the discovering/reporting party MUST ensure that the incident is reported to the grid security contacts. The discovering or reporting party (if not a member of the grid security contacts lists, SHOULD report the incident directly using

security@xxx.yyy

Where xxx.yyy is the name of the grid, e. g. opensciencegrid.org

When reporting via e-mail the following information should be included:

Name:
Phone:
Alternate phone:
E-mail address:
Grid Virtual Organization (VO):
Has your grid identity been compromised?
Description, including time(s), systems involved, and description:
Additional information, e. g. contacts, etc.

6.2. Initial analysis and classification

The reporting contact analyses the incident and provides a severity classification according to:

High: (team leader required)

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

Medium: (team leader required if widespread)

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

Low: (team leader probably not required)

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

This classification should be noted in the report Subject: line to provide a rapid summary of currently understood severity.

6.3. Containment

There are three areas of concern for containment of an attack: (1) preventing further spread of the attack through local services or resources; (2) preventing further attacks from external grid services or resources; and (3) protecting the grid from attacks sourced at a different site. For this discussion, we will assume the local site already has procedures in place to handle (1).

6.3.1. Protection from attacks through the grid

Attacks originating from the grid might be coming from (1) a grid service hosted at the local site; (2) a grid service hosted at a remote site; (3) a shared authentication (group account where some other process possibly at some other site has handled the authentication and authorization of the user to request this resource/service); and (4) a single grid user. As a general matter, the level of response must take into account a number of factors:

- the resource/service has been compromised or is it just under attack?
- the kind of attack - DOS or user or privileged user compromise?
- the importance of the resource/service locally?
- the importance of the resource/service to the operation of the grid?
- the importance of the resource/service to various Virtual Organizations?

As an operational principle for the site, the normal response should probably be to block access from the grid during the initial stages of dealing with an intrusion – only opening access as is prudent and justified, without extraordinary risk. Having this policy results in two beneficial effects: (1) it gives sites more freedom of action and more confidence they can act to protect themselves without bringing down the wrath of the grid community; and (2) it will hopefully result in more redundancy of services, better failover, and applications that are more robust to outages in various parts of the grid (by putting the responsibility on the middleware and application developers to design a more failsafe environment).

Sites SHOULD inform the grid operations center of actions they take affecting grid resources/services.

For group and single user accounts, the initial response is probably the same – temporarily deny access to the resource or service through the appropriate local control on authorization that MUST be provided. In the case of the group account, the follow-up action is different since the service that provides for the "grouping" must be contacted to they can perform corrective actions before the group is re-enabled. In the single user case the follow-up action goes directly back to the VO for resolution.

6.3.2. Protection of the grid from attacks through a site

Many of the considerations from the above discussion also apply here. One would like to believe that grid operations centers would generally have the ability to block a site or service that was misbehaving, and while that might be true in cases for specific centrally controlled middleware services, it will not be true for the vast majority of services on the grid nor will it be true for federated grids that have their own operations centers.

A problematic site or service might be reported by a site on the grid, a grid operations center, site or ISP on another grid or independent of grids, or might be discovered by the monitoring capabilities of the grid operations center.

Depending on the severity of the attack and based on the sites potentially affected, the grid operations center or team leader (or designate) will attempt to notify site, resource and service providers so they can take appropriate action to protect themselves.

The second phase of containment is the process of narrowing down the things that are blocked to the specific sites, resources, services and users which were compromised. Incident response teams at the sites, in communication with their peers through the established email list, are expected to restore normal operation as quickly as the problem areas can be identified and isolated.

6.4. Notification and escalation

For incidents requiring a team leader, an alert MUST be posted to a management list as specified by the governing body for the grid. The team leader SHOULD produce subsequent status reports suitable for management consumption.

6.5. Analysis and Response

6.5.1. Resource tracking

Since the total cost of the incident is often important for legal action, sites should bear in mind during incident response that the incident response costs SHOULD be documented, including:

- responder(s)
- containment actions taken
- what was determined
- what steps taken to respond/recover
- what was the extent of damage
- person-hours required in response

6.5.2. Evidence collection

Documented site procedures for evidence collection and storage are followed (see section 3.2.2).

6.5.3. Removal and recovery

Determine the extent of known and potential compromise of user and host credentials and passwords. Did the initial containment step treat the entire scope of the compromise? Work with contacts to revoke/suspend credentials, keys and passwords. Regular communications of status and observations to the incident discussion mailing list aid in the coordinated recovery.

6.6. Post-Incident Analysis

At the end of an incident, the team leader schedules a conference call to review the lessons learned and formulate feedback to appropriate groups (e. g. grid participants, management, developers). A close-out report MUST be completed within 1 month following the incident.

7. Guidance to middleware and grid service developers

Middleware and grid services should be secure and facilitate security incident analysis and response. At the initial draft of this document, methods and policies are needed for suspension of identities, and richer logging is required throughout middleware and services.

For a grid service/resource hosted at the local site, it MUST have an interface allowing it to be disabled and SHOULD be able to inform central scheduling and monitors that it is entering a disabled state. It is assumed that local site policies will handle containment issues from locally hosted resources/services to the rest of their infrastructure.

For a grid service/resource hosted at a remote site, and interface MUST be provided to local services and resources to block requests or access from the remote service. If a compromise-style of attack then blocking authorizations at the appropriate level is probably sufficient. Queries from remote monitors and schedulers SHOULD be told that access is blocked at the appropriate level. For DOS-style attacks, lower-level protocol blocking is likely to be necessary but there SHOULD still be a way to inform schedulers and monitors that access is being blocked.

8. References and other works

DOE Grids PKI Service
DOE Grids Certificate Policy and Certification Practice Statement
Guidelines for Security Incident Response and Resolution

http://www.doegrids.org/Docs/CP-CPS.pdf

EGEE JRA3: Security

http://egee-jra3.web.cern.ch/egee-jra3/index.html

EGEE Global Security Architecture (EU Deliverable DJRA3.1)
section: Security Considerations: Incident Response

https://edms.cern.ch/document/487004/

LCG Joint Security Group

http://proj-lcg-security.web.cern.ch/proj-lcg-security/

JSG Incident Response Activity

http://proj-lcg-security.web.cern.ch/proj-lcg-security/incident_response.html

Agreement on Incident Response For LCG-1

https://edms.cern.ch/file/428035/LAST_RELEASED/LCG_Incident_Response.pdf

Grid Security Incident definition and exchange format

https://edms.cern.ch/document/501422/1

9. Relevant and related standards and practices

RFC 2350 - Expectations for Computer Security Incident Response

RFC 2196 - Site Security Handbook

RFC 3013 – Guidelines for Evidence Collection and Archiving

IETF Extended Incident Handling (INCH)

http://www.ietf.org/html.charters/inch-charter.html

IETF Incident Object Description Exchange Format (IODEF)

http://www.ietf.org/internet-drafts/draft-ietf-inch-implement-00.txt

LCG Security Group, Agreement on Incident Response

https://edms.cern.ch/file/428035/LAST_RELEASED/LCG_Incident_Response.pdf

CERT/CC - Handbook for Computer Security Incident Response Teams

http://www.cert.org/archive/pdf/csirt-handbook.pdf

CERT/CC - Incident Reporting Guidelines

http://www.cert.org/tech_tips/incident_reporting.html

CERT/CC - Creating a Computer Security Incident Response Team:
A Process for Getting Started

http://www.cert.org/csirts/Creating-A-CSIRT.html

CERT/CC - State of the Practice of Computer Security Incident Response Teams (CSIRTs)

http://www.cert.org/archive/pdf/03tr001.pdf