LCG/EGEE Grid Security Incident Response Handbook

First DRAFT August 2005

Part I Quick Start Guide

Basic guide to minimum steps in grid incident handling.

Part II Grid resources for incident handling

Links to contact points and other information sources.

Part III Grid Services security reference

Service by Service quick reference to assist in incident severity classification

Part IV Incident Playbook.

Incident scenarios described are not intended to be definitive, provide complete coverage of the area or to be used as checklists. They are provided as a basic framework which can discussed, developed and adapted or even discarded as appropriate for particular circumstances.

Read this first.

The target audience for this handbook is grid site security personnel and grid service administrators. It is intended to cover BOTH *LCG* and *EGEE* projects and readers should consider all links, email addresses and other resources quoted as relevant for both projects.

Creative comments and suggestions are welcomed by the editor: ian.neilson@cern.ch

PART I: Quick Start Guide

or

"I think there's something bad happening, what should I do?"

Don't panic: of course you're far too experienced to do that anyway. The first thing for you to do is to report the incident. Reporting gives others the opportunity to protect themselves and allows them to help you if necessary.

Note: Making accurate notes as you handle the incident will be invaluable both during the incident and for post-mortem analysis. Include the times of events in your notes.

There is no one best way to act, but the basic process you should follow is summarized in the following sequence which is described in more detail in the sections below.

Classify
Decide on severity rating for your initial report.

Collate
Gather necessary information for your initial report.

Report
Send your report to the Grid Incident Response list.

Contain
Prevent the incident spreading, protect your site and others.

Analysis & Response
Appropriate actions to resolve the incident.

Post-Mortem
Learn lessons and publish.

Classify:

You should estimate the severity of the incident. Part III of this document is intended to help with this step.

- **HIGH** severity: it seems likely that a significant part of the grid could be made unusable or a significant number of grid identities have been, or may be at risk of compromise.
- **MEDIUM** severity: the event is local to a single grid service (such as a local root compromise) and is unlikely to propagate further.
- **LOW** severity: events affecting local resources and non-privileged accounts.
- Events NOT involving grid resources or identities should be reported using local site procedures. Do not use Grid reporting channels for these events.

Collate:

Gather as much information as you can:

```
Your Name:
Grid Site (as registered in GOCDB):
Contact Phone:
Alternate phone:
E-mail address:
Grid Virtual Organization (VO):
Certificate DN of any compromised identities:
Time(s) of main events (including timezone):
Systems involved or affected (IP address, FQDN):
```

Report:

Write an email report. It should include:

- The Classification you made above in the mail Subject:

  `Subject: HIGH Severity Grid Incident – description of event`

- All the information you gathered in the Collate stage above.
- A complete description of sequence of events as you understand them.
- A statement of what further action, if any, you will be taking and when you will be taking it.

A template report email is available <HERE>.

Send your email report to your local site incident handling point **AND**

project-lcg-security-csirts@cern.ch
or
project-egee-security-csirts@cern.ch
(they are the same lists).

Containment:

Depending on your understanding of the incident, take appropriate steps to contain the incident such as blocking authorization, halting the affected service, fire-walling, disconnecting the network or power-off to control damage. You may have already taken some steps on incident discovery but these must **not significantly delay the reporting** of the incident and you should be careful not to destroy evidence such as log-files which would lead to a better understanding of the incident. If your understanding of what is happening is poor, or you just don't know what to do, go immediately to the next steps.

Analysis & Response:

IMPORTANT NOTE: The lists given above should ONLY BE USED FOR THE INITIAL REPORT. Subsequent responses **and replies** to the report MUST be posted to

After the initial incident report, the course that handling will take depends on many factors. For all HIGH severity and those MEDIUM severity events which have widespread effects, a small team should be assembled to coordinate incident handling. It is the responsibility of the reporting site security contacts and their ROC security contact to put this team in place.

Post-mortem:

You should plan to obtain as full an understanding of what happened as possible and report this to .

project-lcg-security-contacts@cern.ch
or
project-egee-security-contacts@cern.ch
(they are the same lists).

PART II

Grid resources for incident handling

Gather the following information:

Your local security contact/incident handling address: _____

Your ROC security contact address: _____

The LCG/EGEE Security Contacts List.

ROC Security contacts can be reached through the mailing list project-lcg-security-support@cern.ch and project-egee-security-support@cern.ch

Site contact information is maintained in the GOCDB: https://goc.grid-support.ac.uk/gridsite/gocdb2/index.php (check that your site information is accurate)

A list of VO and other contact points is maintained here:
http://lcg.web.cern.ch/LCG/activities/security/contacts.html

A list of CA contact points is maintained here:
http://lcg.web.cern.ch/LCG/users/registration/certificate.html

Contacting a user *(this needs to be improved)*:

a) The user's email address may be in the certificate or proxy being used.
b) The appropriate VO manager (see contacts above).
c) LHC Experiment users are registered in the PIE database:
http://greybook.cern.ch/

LCG/EGEE approved Incident Response Policy is located at https://edms.cern.ch/document/428035/LAST_RELEASED (Since policy approval can be a slow process, the current draft version (if applicable) should also be consulted and is always here: https://edms.cern.ch/document/428035)

LCG/EGEE security policy documents are managed by the Joint Security Policy Group (JSPG) and are available for reference at http://proj-lcg-security.web.cern.ch/proj-lcg-security/

PART III

Grid Services security reference

Based on the LCG2 Manual Installation Guide, the following node types are defined:

Information System

BDII

Workload Management System

Resource Broker
Computing Element (Torque)
Worker Node (Torque)

Data Management System

LFC Server (mysql)
Classical Storage Element (SE classic)

DPM Storage Element (SE dpm mysql)
DPM Disk server (SE dpm disk)
dCache Storage Element (SE dcache)

VO, Security, Monitoring, Accounting

VOMS
User Interface
Mon Box
Proxy Server
VOBOX for VO agents

PART IV

Incident PlayBook

Case: Local unattributed activity from a single user
Case: Compute Element relaying SPAM
Case: Poisoning of information system

Case: Local unattributed activity from a single user

- Incident Class: LOW
    - Reported by user to GGUS based on accounting
- Actors: GGUS, User, Site
- Response:
    - Report received by SSO from GGUS
- Investigation (Site <-> User)
- Analysis: Single identity compromised
    - Route to compromise may change response
- Notification by SSO: User, VO(suspend), REPORT-L, GGUS
- Issues:
    - How does SSO contact user, VO?
    - 000's of distributed users -> notification overload

Case: Compute Element relaying SPAM

- Incident Class: Medium
    - Reported by external corporate security team
- Actors: Site, Ex-CSIRT
- Response:
    - Report received by SSO from Ex-CSIRT
    - Prelim. Investigation (SSO)
    - Close service, remove from network
    - Notification: REPORT-L, NREN CSIRT
- Analysis: CE rooted
- Notification: DISCUSS-L
- Issues
    - Service-based threat analysis would be useful

Case: Poisoning of information system

- Incident Class: HIGH

    - Reported simultaneously from multiple locations, widespread job misdirection, failure, DOS
- Actors: Multiple Site, Experts, Developers/Deployment
    - + Users, VOs, Management
- Response
    - Reports might start as unassociated REPORT-L posts
    - Team leader created, creates team – Notify: REPORT-L
- Prelim Analysis: logs, network traffic
- Mitigation: network blocking, rebuild/lock IS – Notify: DISCUSS-L
- Analysis: Broken protocol
    - Patch Created, Packaged and Deployed – Notify: Site admin
- Notification: DISCUSS-L
- Issues
    - How to bootstrap team and its leader – ROC/OSCT role
    - Team communications – Incident tracking tools
    - Team communications to developers
    - Deployment scheduling – how long