LCG/EGEE Grid Security Incident Response Handbook

Version 0.4 December 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.

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. For the sake of brevity the LCG acronym has been used throughout. Map from one address to the other by replacing *lcg* with *egee*.

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 prepare and submit a report of incident. Reporting gives others the opportunity to protect themselves and allows them to help you if necessary.

Note: You must make accurate notes as you handle the incident. These 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.

Collate
Gather necessary information for your initial report.

Report
Send your report to the Grid Incident Response list.

The content of the remaining stages will depend on the exact nature of the incident.

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

Analysis & Response
Appropriate actions to resolve the incident.

Post-Mortem
Learn lessons and publish.

At all stages you should be able to get support from your ROC security contacts or from the OSCT through project-lcg-security-support@cern.ch.

Collate:

Gather as much information as you can:

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

You may not have sufficient information but you should try to estimate the severity of the incident as indicated below if possible. Your initial investigation should be quick and focused on gathering accurate information for an initial report. DO NOT DELAY reporting unnecessarily and use a severity of UNKNOWN if you are not sure.

- HIGH severity: it seems likely that a significant part of the external 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.

Report:

Write an email report. It should include:

- All the information you gathered in the Collate stage above.

  Include any classification you made in the mail Subject:

  `Subject: HIGH Severity Grid Incident – description`

- A complete description of sequence of events.
- A statement of what further action, if any, you will be taking and when you will be taking it.

A sample report email is available in Appendix A below.

If possible set the **reply address** of your report to -

project-lcg-security-contacts@cern.ch.

Send the report to –

local site incident handling point AND
project-lcg-security-csirts@cern.ch

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 project-lcg-security-contacts@cern.ch

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

PART II

Grid resources for incident handling

Gather the following information:

Your local site security contact/incident handling address :

Your ROC security contact email address :

Your ROC security contact telephone number :

The LCG/EGEE Security Contacts List (distributed periodically to security contacts).

ROC Security contacts can be reached through the mailing list project-lcg-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)

The EGEE CIC portal provided a tool for contacting site administrators, VO managers and others: https://cic.in2p3.fr/index.php?id=rc&subid=rc_publish&js_status=2 (certificate authentication required)

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

If you support other VOs, make sure you also contact addresses for them.

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

Contacting a user:

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/ (Searchable: http://graybook.cern.ch/ExperimentSearch.html)

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/

Appendix A

Sample initial 'heads-up' incident report:

Sent to project-lcg-security-csirts@cern.ch

Subject: MEDIUM Severity Grid Incident - foo.bar.cern.ch

On DD/MM/YYYY, foo.bar.cern.ch (128.142.xxx.yyy) at CERN was discovered compromised after sending multiple emails.

The machine, which was configured as a CE but not in production use, has been taken offline for investigation.

Initial findings indicate attacker connected on DD'/MM/YYYY from
x.y.z
x.yy.zz
xx.yy.zzz

Further details to follow.

[Name, Institute, telephone and email of reporter supplied]

Sample post-mortem report:

Sent to project-lcg-security-contacts@cern.ch

Subject: MEDIUM Severity Grid Incident - foo.bar.cern.ch

```
******************
*     SUMMARY     *
******************
```

On DD/MM/YYYY, foo.bar.cern.ch (128.142.xxx.yyy) from CERN has been discovered compromised.

The attacker gained access to the system by discovering a legitimate user's password. He/She obtained root access by using a local root exploit against an unpatched Linux kernel.

The machine was configured as a CE but not in production use and there is no evidence that grid credentials have been stolen.

```
******************
*     DETAILS     *
******************
```

On DD'/MM/YYYY, an attacker launched a brute force attack against the SSH daemon running on foo.bar.cern.ch (128.142.xxx.yyy), which was accessible from the Internet. For unclear reasons, the attacker managed to find the password of the existing user "joebar" and used this account to access the system.

On DD''/MM/YYYY, the attacker obtained root privileges on the system. The operating system (Red Hat 7.3) was up-to-date with the Fedora Legacy Community patches, but was running a recompiled Linux 2.4.24 kernel, which included several local root privilege escalation vulnerabilities.

A backdoor and a rootkit (probably SuckIT) have been installed on the system, but there is no indication that grid credentials have been stolen.

On DD''/MM/YYYY, the system has been discovered compromised. Indeed, logwatch output reported a suspicious login of a user who should not exist (haxxor) and a lot of emails were being sent from the system.

A file -- probably generated by a sniffer included in the rootkit -- has been discovered containing hostnames and usernames/passwords. Amongst others, the file was referring to:

* foo1.bar1.edu
* foo2.bar2.edu

The relevant security representatives have been contacted. Both of them responded promptly.

The home directory of the attacker contained more than 50 files, mostly malicious software (exploits, backdoors, trojanised applications, bruteforcers, keyloggers, spam generators).

The attacker logged in from multiple places:
x.y.z
x.yy.zz
xx.yy.zzz

Also, it seems that the attacker copied an old linux virus (Linux.RST.B) in a non-executable text file parameter file on the compromized system, which obviously did not work.

****
* RESOLUTION *
****

A supported operating system (Red Hat Entreprise Linux 3) has been reinstalled on foo.bar.cern.ch and the service it provides has been restored.

As reflected in the GOC DB entry for CERN, the CERB grid service 'foo' has been withdrawn since DD''/MM/YYYY and it is hoped to restore it within 30 days.

Revocation of the host certificate has been requested.

Images of the disks of all systems that were investigated have been kept in case any further analysis is necessary.

The rest of the computer farm is been searched for similar vulnerabilities, but none has been found.

****
* CONTACTS *
****

[Name, Institute, telephone and email of reporter supplied]