Operational Security Coordination Team

LCG/EGEE Incident Response Procedure

Date:	**10 September 2007**
EDMS Reference:	https://edms.cern.ch/document/867454
Internal Version:	**1.0**
Status:	**Released**
Author:	**Romain Wartel, on behalf of the EGEE OSCT**

Document Log			
Issue	**Date**	**Author**	**Comment**
1.0	10 Sept 2007	Romain Wartel	Initial version

1 Introduction

This procedure is provided for guidance only and is aimed at minimising the impact of security incidents, by encouraging post-mortem analysis and promoting cooperation between the sites. It is based on the EGEE Incident Response policy[1].

2 Definition

A security incident is the act of violating an explicit or implied security policy (ex: local security policy, EGEE Acceptable Use Policy[2]).

3 Intended Audience

This document is intended for Grid site security contacts and site administrators.

4 Incident response prodecure

When a security incident is suspected, the following procedure should be used:

1. Contact immediately your local security team and your ROC Security Contact.
2. In case no support is shortly available, whenever feasible and if you are sufficiently familiar with the host/service to take responsibility for this action, try to contain the incident, for instance by unplugging the network cable connected to the host. Do NOT reboot or power off the host.
3. Assist your local security team and your ROC Security Contact to confirm and then announce the incident to all the sites via project-egee-security-csirts@cern.ch.
4. If appropriate:
   - report a downtime for the affected hosts on the GOCDB
   - send an EGEE broadcast announcing the downtime for the affected hosts Use "Security operations in progress" as the reason with no additional detail both for the broadcast and the GOCDB.
5. Perform appropriate forensics and take necessary corrective actions
   - If needed, seek for help from your local security team or from your ROC Security Contact or from project-egee-security-support@cern.ch
   - If relevant, send additional reports containing suspicious patterns, files or evidence that may be of use to other Grid participants to project-egee-security-contacts@cern.ch. NEVER send potentially sensitive information (ex: hosts, IP addresses, usernames) without clearance from your local security team and/or your ROC Security Contact.
6. Coordinate with your local security team and your ROC Security Contact to send an incident closure report within 1 month following the incident, to all

[1] https://edms.cern.ch/file/428035/LAST_RELEASED/Incident_Response_Guide.pdf

[2] https://edms.cern.ch/file/428036/LAST_RELEASED/Grid_AUP.pdf

the sites via project- egee-security-contacts@cern.ch, including lessons learnt and resolution.

7- Restore the service, and if needed, send an EGEE broadcast, update the GOCDB, service documentation and procedures to prevent recurrence as necessary.

5 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