Incident Response Coordination in the Italian Production Grid

Riccardo Brunetti, Luca Dell'Agnello (representing the italian ROC)

Roberto Cecchini (representing the GARR-CERT)

Luca Carbone (representing the CCR)

03/07/08

1 About this document

The purpose of this document is to describe how the security incident response procedures can be coordinated in a computing and network infrastructure which includes Grid projects.

The main notice here is that in a Grid computing environment the way the resources are accessed and administered is changing. The strong sharing of computing and storage resources connected by hight speed networks and the use of Virtual Organization as trust model, is forcing a change on the concept of site security and on the way the incidents must be treated.

When dealing with a security problem in Grids, we should consider that the users involved can be remote (i.e. away from the direct control of the local administrators) and that the resources which are the source of the problem can be hosted by remote sites. At the same time, a local problem can potentially have implication in many other Grid sites.

Finally, another problem to consider is that the management of Grid sites is often under the responsibility of staff people who are not part of the team which is responsible for the administration of the general-purpose computing resources and services.

For these reasons, a good coordination of the incident response procedures needs to involve a number of different teams: local site administrators, Grid services administrators (if different from the previous) and people responsible for the security of the national network infrastructure (GARR[1]-CERT[2]) and Grid coordination

1 **GARR**: Gestione Ampliamento Rete Ricerca
2 **CERT**: Computer Emergency Response Team

(ROC[3]).

The security procedures herein described have been reviewed to improve the communication between network and site administrators and EGEE computing resource administrators.

This review involved people[4] representing the Italian ROC, the INFN computing committee and the GARR-CERT.

2 Actors

2.1 Network Infrastructure Level

- *GARR-CERT*: Computer Emergency Response Team for GARR

2.2 ROC Level

- *ROC_Italy CSIRT*[5]: A group of people (at least 2), reachable through the mailing list grid-security@infn.it, responsible for the security coordination inside the ROC
- *ROC_Italy Security Officer (RSO)*: A single person responsible for the security coordination inside the ROC. It MUST be a member of the ROC_Italy CSIRT.

2.3 Site Level

- Local Site Managers (LSM): People responsible for the management of the networking and computing resources at a site.
- *Access Point Manager (APM)*: The GARR contact person who is responsible for the management of the top level access router and IP addresses assignment. A APM is present at all sites.
- Grid Site Managers (GSM): People responsible for the management of the grid services and resources at a site.
- *grid Site CSIRT* (gCSIRT): A group of people (at least 2), reachable through the mailing list (grid-sec@...site.....), responsible for the security incident support on grid resources. It MUST exist in every site and MUST include at least one Grid Site Manager.

---

3 **ROC**: Regional Operation Center. The ROC provides operations support, acting as Grid Operations Centers in analogy with Network Operations Centers (NOCs). It also provides operational and performance monitoring, troubleshooting, etc. as well as general grid services such as VO-related services.

4 Riccardo Brunetti (ROC_Italy), Luca Carbone (INFN CCR), Roberto Cecchini (GARR CERT), Luca Dell'Agnello (ROC_Italy)

5 **CSIRT**: Computer Security Incident Response Team

- *grid Site Security Officer (gSSO)*: A single person responsible for the security coordination on grid resources. It MUST exist in every site and MUST be a member of the grid Site CSIRT.

3 Use cases

Given the actors defined above, we considered the following use cases:

3.1 An incident is discovered by a Local Site Manager

3.1.1 The LSM alerts immediately the APM.

3.1.2 The APM escalates the alert to the GARR CERT and start to follow the GARR incident response procedures.

3.1.3 If some host is involved which is related to the Grid environment, the APM alerts immediately the site gCSIRT (the gSSO, as a member of the gCSIRT, receives the alert)

3.1.4 The gSSO escalates the alert to project-egee-security-csirts@cern.ch and to grid-security@infn.it (the RSO receives the alert) and starts to follow the EGEE incident response procedure, in coordination with the APM.

3.2 An incident is discovered by a Grid Site Manager

3.2.1 The GSM alerts immediately the site gCSIRT (the gSSO receives the alert)

3.2.2 The gSSO escalates the alert to project-egee-security-csirts@cern.ch and to grid-security@infn.it (the RSO receives the alert) and starts to follow the EGEE incident response procedure.

3.2.3 If the incident may affect the integrity of the local computing infrastructure, the gSSO alerts the APM

3.2.4 The APM escalates the alert to the GARR-CERT and starts to follow the GARR-CERT incident response procedure in coordination with the gSSO.

3.3 An incident is discovered from outside the site

3.3.1 A generic incident is reported to the APM. The APM will receive the alert and the flow will be the same as ***3.1*** above from point 3.1.2

3.3.2 The gCSIRT is notified about a security problem related to the site. In this case the flow will be the same as ***3.2*** above from point 3.2.2

4 Incident Response Procedures

The following procedures will be adopted in incident handling:

1. GARR-CERT procedures:

   http://www.cert.garr.it/incidenti-en.php3

2. EGEE procedures:

   https://edms.cern.ch/file/867454/LAST_RELEASED/EGEE_Incident_Response_Procedure.pdf

   http://proj-lcg-security.web.cern.ch/proj-lcg-security/docs/LCG_Incident_Response.asp

5 Incident Response Activity Diagram