ROC Security Contacts

R. Rumler
Lyon/Villeurbanne

Contents

- Security contact: implied entities
- Procedures
- Documentation and communication

Security contacts: entities (1)

- **Operational Security Coordination Team - OSCT**
  - Composed of all ROC security contacts plus the EGEE Security Officer
  - Discussion list: project-egee-security-support
  - Role
    - Forward initial information about an incident
    - Create an intervention team if necessary
  - OSCT- duty contact (OSCT-DC): associated to COD team
- **Grid Security Vulnerability Group**
  - Members named by the project
  - Contact to signal a (supposed) vulnerability: grid-vulnerability-report
  - Role
    - Analyse the middleware and other programs used in the context of the grid to find potential vulnerabilities
    - Determine the degree of risk (Risk Analysis Team - RAT)
    - Develop a recommendation about the action(s) to be taken

Security contacts: entities (2)

- **Computer Security Incident Response Team - CSIRT**
  - Distribution lists:
    - Discussion: project-egee-security-contacts
    - Signal an incident: project-egee-security-csirts

  The security contacts registered in the GOCDB serve to constitute those lists.
- **GGUS support unit: Security**

  Security incidents or information requests can be signalled through GGUS. One can create a ticket and assign it to the Security support unit.

  Attention: all GGUS tickets are publicly readable, so confidential data or contact information should not be mentioned there.
- **CIC-on-Duty - COD**

  The grid operator can open security tickets in GGUS, monitors GGUS for this kind of tickets and has the obligation to invoke the OSCT duty contact (OSCT-DC) when such a ticket appears or a security incident happens.

  The COD can suspend sites immediately on demand from the EGEE security officer.

Procedures

- In case of a security incident detected by a grid site, this site must inform its ROC.
- In all cases, the site has to follow the local security rules and procedures in terms of information of other authorities and of incident analysis.
- The grid procedures have to be applied in addition to and not instead of the local ones.

- The ROC informs its security contact (= its OSCT member) or directly the OSCT.
- The OSCT creates an intervention team if appropriate (in addition to the one which might already be in place according to the local security procedures); in principle the ROC and the site having the incident should take the initiative to create the team. Anyway, the OSCT-DC has this role by default.

Documentation

- **JSPG policy documents**
  http://proj-lcg-security.web.cern.ch/proj-lcg-security/documents2.html
- **Current OSCT website**
  https://twiki.cern.ch/twiki/bin/view/LCG/OSCT
- **New OSCT website (nearly completed construction)**
  http://osct.web.cern.ch/osct/n/
- **Incident response guide**
  https://edms.cern.ch/file/428035/LAST_RELEASED/Incident_Response_Guide.pdf