EGI CSIRT Security Incident Handling Procedure

Vincent Brillault, CERN, EGI-CSIRT

Policy update

EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142

What is it, why an update?

EGI CSIRT Security Incident Handling Procedure

- Covers:
  - Sites expected response during incident
  - EGI-CSIRT role and responsibility during incidents
- Issues:
  - Missing few parts concerning the EGI FedCloud
  - Unclear actions/asked to the wrong person
  - Was a Word/PDF document

What's new?

- Minor rewording in every section
- Resource Centers asked to:
  - not delete compromised VMs
  - identify VAs used by compromised VMs
- EGI-CSIRT now clearly responsible for:
  - Reporting compromised users to VO & CAs
  - Coordinating response for vulnerable VAs
  - Send closure report

Resource Center Responsibilities

1. Within 4 hours of discovery: Inform your local security team, your NGI Security Officer and the EGI CSIRT via abuse@egi.eu. You are encouraged to use the recommended templates

2. Within 1 day of isolation: Contain the incident while as far as possible preserving forensic data: Do NOT reboot or power off hosts. Do NOT destroy VMs. Isolate the compromised systems. Do NOT disconnect them from the network, unless you have to. If possible take a snapshot of the compromised systems. Consult with your local security team and the EGI CSIRT.

Resource Center Responsibilities

3. Together with your local security team and the EGI CSIRT decide if it is an incident that requires further investigation or action.

4. Within 1 day of discovery: If applicable, announce downtime for the affected services in accordance with the EGI Operational Procedures

5. Within 4 working hours of any EGI CSIRT request: Perform appropriate analysis and take necessary corrective actions, see Incident Analysis Guideline

Resource Center Responsibilities

6. Within 1 month of incident resolution: Coordinate with your local security team and the EGI CSIRT to send an incident closure report to the EGI CSIRT via abuse@egi.eu, including lessons learnt and resolution. This report should be labelled AMBER or RED, according to the Traffic Light Protocol.

7. Restore the service and, if needed, update the service documentation and procedures to prevent recurrence as necessary.

Incident Analysis Guideline Information expected

- Who/how detected or reported the incident
- Host(s) affected (ex: compromised hosts, hosts running suspicious user code)
- Evidence of the compromise, including timestamps (ex: suspicious files, log entry or network activity)
- The actions taken to resolve the incident

Incident Analysis Guideline When applicable/available

- Possibly affected X509 certificate DNs of the user(s), operator(s), consumer(s)
- Host(s) used as a local entry point to the RC (ex: UI or WMS IP address)
- Remote IP address(es) of the attacker
- The virtual appliance used to instantiate any affected virtual machine.
- What was lost, details of the attack (ex: compromised credentials, (root) compromised host)
- Any remote IP you suspect to be affected
- Vulnerabilities possibly exploited by the attacker

EGI-CSIRT Responsibilities

- Name/Regroup incidents
- Actively ask for response
- Help RCs (e.g. recommendations)
- Maintain communication with third parties
- Send updates and final report
- (Un-)Suspend users, notify VOs and CAs
- De-endorse VAs, contact sites supporting them

EGI CSIRT Security Incident Handling Procedure

- Full procedure in the wiki as SEC01
- One-page check-list: print it!
- Now waiting for your approval!