SEC01 EGI CSIRT Security Incident Handling Procedure

Document control

Area	ISM
Procedure status	FINAL
Owner	CSIRT
Approvers	OMB
Approval status	APPROVED
Approved version and date	31 Mar 2016
Statement	This procedure is aimed at minimising the impact of security incidents by encouraging post-mortem analysis and promoting cooperation between Resource Centres.
Dissemination Level	TLP:WHITE - Public

Procedure reviews

The following table is updated after every review of this procedure.

Date	Review by	Summary of results	Follow-up actions / Comments
21 Oct 2021	Baptiste Grenier	Import from EGI wiki	

Table of contents

Overview

This procedure is aimed at minimising the impact of security incidents by encouraging post-mortem analysis and promoting cooperation between Resource Centres.
It is based on the Security Incident Response Policy.

This incident response procedure is aiming at complementing local security procedures. Unless specified otherwise in separate service level agreements, all times in this document refer to normal local working hours.

This document is intended for Resource Center security contacts and administrators and is primarily aimed at reporting, investigating and resolving security incidents.

Previous approved version of the procedure - *approved*, July 2010 (MS405)

Definitions

Please refer to the EGI Glossary for the definitions of the terms used in this procedure.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", “MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Entities involved in the procedure

- **EGI-CSIRT Security Officer on Duty**: irtf at mailman.egi.eu
- **NGI Security Officer**: NGI Security E-Mail as defined in Configuration Database
- **Resource Center**: RC CSIRT E-Mail as defined in Configuration Database

Contact points

- **abuse at egi.eu**: Address to be used for reporting security Incident (In case of TLP:RED data, use GPG: A97F 3BDD F0EE 01A1 176C C13A 93BF 7F91 5696 F750)
- **site-security-contacts at mailman.egi.eu**: Mailing list containing all Resource Center "CSIRT E-Mail" as defined in Configuration Database
- **ngi-security-contacts at mailman.egi.eu**: Mailing list containing all NGI "Security E-Mail" as defined in Configuration Database

Triggers

A Security incident has been identified.

Resource Center Responsibilities

The following table describes the actions to be taken when an incident potentially affecting EGI users, data, services, infrastructure is **suspected**. Administrators are recommended to take note of every action (with timestamp) they take, for later analysis or legal cases.

Step	Action	Deadline
1	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.	Within 4 hours of discovery
2	In consultation with your local security team and the EGI CSIRT, act to isolate the compromised systems and contain the incident whilst preserving forensic data. Take a snapshot of affected VMs. Isolate at the network level if possible. Do NOT reboot or power off hosts. Do NOT destroy VMs. Physically disconnect systems from the network ONLY where other options are not available.	Within 1 day of discovery
3	Together with your local security team and the EGI CSIRT decide if it is an incident that requires further investigation or action.	
4	If applicable, announce downtime for the affected services in accordance with the EGI Operational Procedures	Within 1 day of isolation
5	Perform appropriate analysis and take necessary corrective actions, see Incident Analysis Guideline	Within 4 working hours of any EGI CSIRT request
6	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.	Within 1 month of incident resolution
7	Restore the service and, if needed, update the service documentation and procedures to prevent recurrence as necessary.	

Resource Centre Checklist

EGI-CSIRT Responsibilities

EGI-CSIRT Security Officer on Duty

The EGI-CSIRT Security Officer on Duty tasks are:

- Evaluate the initial incident report and determine whether it appears to be part of an incident covering multiple RCs, in particular, whether it is related to a previously known incident (e.g. do the same attacking IP addresses appear, are the attacker's tools and methodology strongly similar):
  - If this is a new, unrelated incident, assign an identifying tag (of the format [EGI-YYYYMMDD-NN]) to the incident and announce it to all RCs via site-security-contacts@mailman.egi.eu, all NGIs via ngi-security-contacts@mailman.egi.eu and the EGI CSIRT via csirt@egi.eu using the recommended templates.
  - If the incident is part of an incident covering multiple RCs, the incident coordinator MAY choose not to announce each incident separately, but instead issue regular updates on the overall incident.
- Take any appropriate actions in order to:
  - Contact affected parties to obtain accurate information at an appropriate level of detail and in a timely manner.
  - Investigate to determine the cause and extent of the incident, what assets have been compromised (credentials etc.), and how to resolve the incident.
  - Help involved RCs to resolve the incident by providing recommendations, promoting collaboration with other RCs and periodically checking their statuses.
  - Maintain communications with any other involved parties inside and outside EGI.
- When appropriate, send updated:
  - Summary reports to all RCs, NGIs and the EGI-CSIRT (site-security-contacts@mailman.egi.eu, ngi-security-contacts@mailman.egi.eu an csirt@egi.eu), containing the status of the incident and indicators of compromise that can be used by RCs to evaluate their implication
  - Detailed reports to the RCs directly involved and affected by the incident, containing interesting findings or possible leads that could be used to resolve the incident
- If malicious behaviour or a policy violation can be linked to a user account or identity:
  - Add the account or identity to the emergency suspension list following the appropriate procedure.
  - If applicable, report the incident to the VO providing access. Coordinate any user suspension and job termination with the VO.
  - Without hindering the investigation, verify the legitimacy or otherwise of the activity with the owner of the account or identity
- If user credentials have been exposed or compromised, report it to the relevant credential provider. In particular, CA contacts are available on https://www.eugridpma.org/showca.
- When suspended accounts or identities no longer represent a threat, typically when the incident is resolved and compromised credentials have been re-issued, remove them from the emergency suspension list
- When a virtual appliance is identified as being vulnerable or malicious, ensure that:
  - Its endorsement is revoked on APP-DB
  - All instantiated and running VMs using this virtual appliance are properly handled
- Based on the incident closure report received from the affected RC, send a closure report with the relevant information to all partners.

EGI-CSIRT Security Incident Coordinator

In addition, the EGI CSIRT appoints a security incident coordinator for each incident, responsible for:

- Ensuring that the investigation does not stall
- Ensuring that information is properly logged
- Conducting a debriefing after the investigation is complete.

Incident Analysis Guideline

As part of the security incident resolution process, RCs are expected to produce the following information:

- 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
- 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
    - Details of malicious jobs, in particular: submitter, submission time, start time, local job ID, hostname/IP

RCs are also expected to:

- Report any action taken to the EGI CSIRT as often as necessary
- Identify and kill suspicious process(es) as appropriate, but aim at preserving the information they could have generated, both in memory and on disk by dumping them beforehand, see Forensics Howto.
- If it is suspected that any credentials have been abused or compromised, you MUST inform the EGI CSIRT who take appropriate action. Inform the EGI CSIRT of any direct contact with the involved VO, CA or any other credential provider.
- If it is suspected that a virtual appliance used to instantiate an affected virtual machine is vulnerable or malicious, you MUST report it to the EGI CSIRT.
- Seek help from your local security team, from your NGI Security Officer or from the EGI CSIRT
- If relevant, additional reports containing suspicious patterns, IP addresses, files or evidence that may be of use to other infrastructure parties SHOULD be sent to the EGI CSIRT.

RCs are also recommended to:

- Locally suspend any credential that has been directly reported to be violating the AUP. Unless emergencies, serious risks or damages, non-responsiveness of the VO or recommended otherwise, sites are not recommended to immediately suspend VO's pilot DNs indirectly (user payload) violating the AUP.

As part of the investigations, RCs MUST be able to provide the relevant logging information produced by local services. Logging information such as IP addresses, timestamps and identities involved etc., concerning the source of any suspicious successful connection, must meet the following minimal requirements, if possible according to local laws:

- 6 months prior to the discovery of the incident for successful SSH connections against EGI services, and for the originating submission host for grid jobs or virtual machines
- 3 months prior to the discovery of the incident for all other EGI related services.