EGI-InSPIRE

OPERATIONAL SECURITY PROCEDURES

EU MILESTONE: MS412

Document identifier:	EGI-MS412-V2.3.doc
Date:	**24/08/2011**
Activity:	**SA1**
Lead Partner:	**CNRS**
Document Status:	**FINAL**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/649

Abstract

To ensure the sustainability of a deployed grid infrastructure it is important that it is sufficiently secure. This document is the entry point to the EGI operational security procedure framework. It aims to give an overview of operational security processes.

I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	Dorine Fouossong	CNRS	30/6/2011
Reviewed by	**Moderator:** Stuart Kenny **Reviewers:** Michel Drescher	NA3/TCD SA2/EGI.eu	4/8/2011
Approved by	**AMB & PMB**		24/8/2011

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	30/06/2011	First draft after EGI-CSIRT internal discussions	Dorine Fouossong/CNRS
2	08/07/2011	Second draft after an internal review meeting	Dorine Fouossong/CNRS
3	11/07/2011	Adapted to EGI template	Dorine Fouossong/CNRS
4	13/07/2011	Sections extended	Dorine Fouossong/CNRS
5	18/07/2011	Addressing comments from Ursula Epting	Dorine Fouossong/CNRS
6	19/07/2011	Addressing comments from Linda Cornwall and Riccardo Brunetti	Dorine Fouossong/CNRS
7	22/07/2011	Addressing comments from noc-managers and SPG	Dorine Fouossong/CNRS
8	27/07/2011	Addressing comments from Peter solagna	Dorine Fouossong/CNRS
9	31/07/2011	First pass with external reviewers	Dorine Fouossong/CNRS
10	05/08/2011	Updating the link to approved documents	Dorine Fouossong/CNRS

IV. APPLICATION AREA

This document is a formal deliverable for the European Commission, applicable to all members of the EGI-InSPIRE project, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

V. DOCUMENT AMENDMENT PROCEDURE

Amendments, comments and suggestions should be sent to the authors. The procedures documented in the EGI-InSPIRE "Document Management Procedure" will be followed:
https://wiki.egi.eu/wiki/Procedures

VI. TERMINOLOGY

A complete project glossary is provided at the following page: http://www.egi.eu/about/glossary/.

VII. PROJECT SUMMARY

To support science and innovation, a lasting operational model for e-Science is needed − both for coordinating the infrastructure and for delivering integrated services that cross national borders.

The EGI-InSPIRE project will support the transition from a project-based system to a sustainable pan-European e-Infrastructure, by supporting ‘grids’ of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI-InSPIRE will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop grids, to benefit user communities within the European Research Area.

EGI-InSPIRE will collect user requirements and provide support for the current and potential new user communities, for example within the ESFRI projects. Additional support will also be given to the current heavy users of the infrastructure, such as high energy physics, computational chemistry and life sciences, as they move their critical services and tools from a centralised support model to one driven by their own individual communities.

The objectives of the project are:

1. The continued operation and expansion of today’s production infrastructure by transitioning to a governance model and operational infrastructure that can be increasingly sustained outside of specific project funding.
2. The continued support of researchers within Europe and their international collaborators that are using the current production infrastructure.
3. The support for current heavy users of the infrastructure in earth science, astronomy and astrophysics, fusion, computational chemistry and materials science technology, life sciences and high energy physics as they move to sustainable support models for their own communities.
4. Interfaces that expand access to new user communities including new potential heavy users of the infrastructure from the ESFRI projects.
5. Mechanisms to integrate existing infrastructure providers in Europe and around the world into the production infrastructure, so as to provide transparent access to all authorised users.
6. Establish processes and procedures to allow the integration of new DCI technologies (e.g. clouds, volunteer desktop grids) and heterogeneous resources (e.g. HTC and HPC) into a seamless production infrastructure as they mature and demonstrate value to the EGI community.

The EGI community is a federation of independent national and community resource providers, whose resources support specific research communities and international collaborators both within Europe and worldwide. EGI.eu, coordinator of EGI-InSPIRE, brings together partner institutions established within the community to provide a set of essential human and technical services that enable secure integrated access to distributed resources on behalf of the community.

The production infrastructure supports Virtual Research Communities (VRCs) − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

VIII. EXECUTIVE SUMMARY

This document is the second yearly report on security related operational procedures for handling incidents and vulnerabilities.

Whereas MS405[1], its predecessor provides two detailed documents, MS412 offers a synthetic view of operational security procedures in one unique document.

It will cover three procedures:

- Security incident handling,
- Security vulnerability issue handling,
- And critical vulnerability handling.

The first two are older as there was approved as part of MS405. The main evolution since last year and MS405 is the third one, critical vulnerability handling procedure which was approved in March 2011.

The three procedures described in the document are related each other as they contribute to increase the security of EGI Infrastructure. The second procedure may in some cases raise the third one but, the three processes are autonomous and separated.

The approved releases of these procedures are available at: https://wiki.egi.eu/wiki/Operational_Procedures#Security .

[1] https://documents.egi.eu/document/47

TABLE OF CONTENTS

1 INTRODUCTION

To cover user needs for high storage and computational capacities, the grid infrastructure offers distributed computing resources that are controlled by many different institutions. In order to allow this, a cross-organizational structure for resources operations is needed.

This document describes the operational processes in place, which contribute to achieve day-to-day security of EGI's grid infrastructure.

The activities described in this document are part of the WP4 "SA1 – operations" of EGI-InSPIRE Document of Work; this work package coordinates the providing of a secure and reliable European-wide production grid infrastructure federated from national grid initiatives. They are regulated by policies defined by the EGI Security Policy Group. Lessons learned from day-to-day security operations are raised to the EGI Security Policy Group and vice versa. This is done through a collaborative body called EGI Security Coordination Group.

Operational security tasks are led by EGI Computer Security Incident Response Team, and EGI Software Vulnerability Group; they involve security teams from sites and National Grid Infrastructure.

The intended audience of this document is all EGI stakeholders.

2 SECURITY INCIDENT HANDLING

2.1 Purpose and scope

The aim of the incident handling process is to deal with a security incident potentially affecting grid users, services or operations.

The EGI's procedure aims to minimize the impact on the infrastructure by encouraging post-mortem analysis and promoting cooperation between sites.

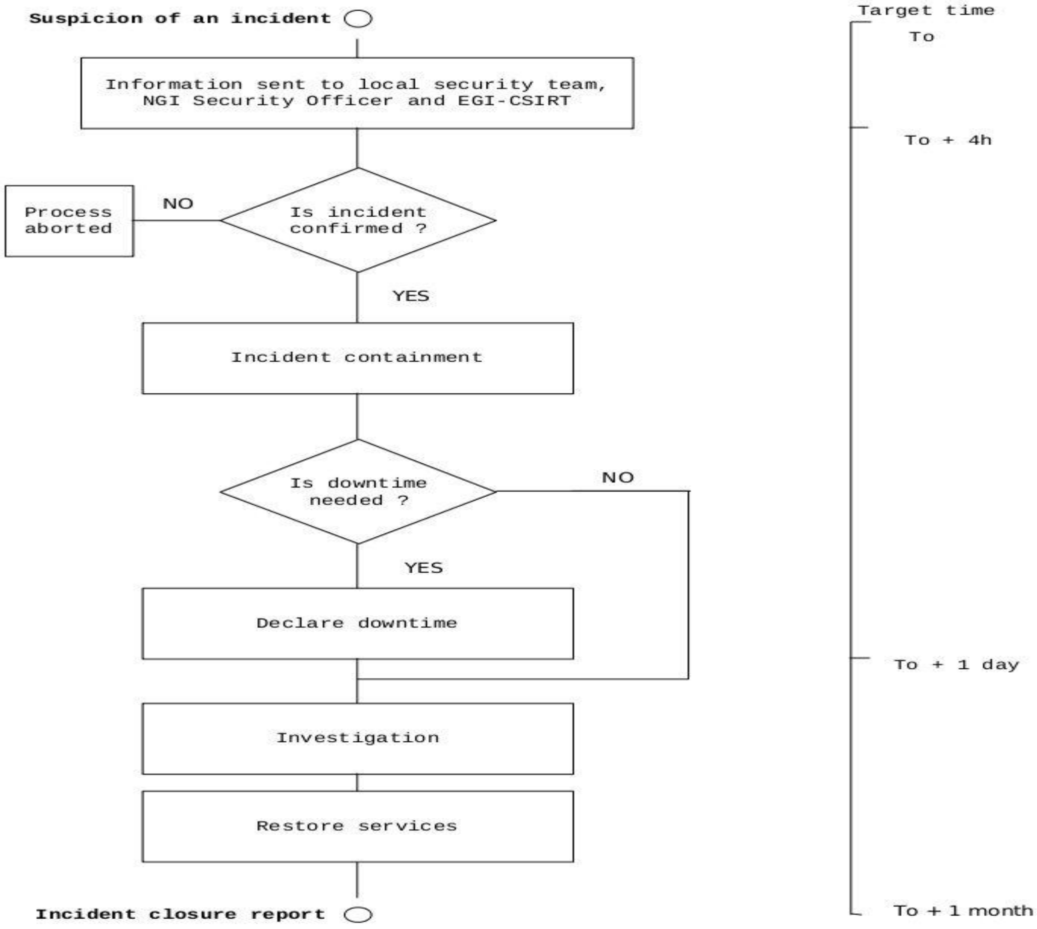
2.2 People involved

The overall process coordination is under the responsibility of EGI-CSIRT.

The EGI-CSIRT main goal is to understand the causes of the incidents and to limit their impact on the EGI infrastructure. The EGI CSIRT Incident Response Task Force appoints a security incident coordinator for each incident. The incident coordinator assists affected sites in the process to resolve the incident, and maintains communication with involved parties.

On the NGI's side, the main actors are NGI CSIRT and Site CSIRT. The Site CSIRT's role is to detect, contain and investigate the incident if relevant. Sites should communicate with the EGI-CSIRT in a timely manner. The NGI-CSIRT should actively stimulate sites within its NGI. Sites can request help from their local security experts, their NGI-CSIRT and from EGI-CSIRT itself.

2.3 Main steps



3 SECURITY VULNERABILITY ISSUE HANDLING

3.1 Purpose and scope

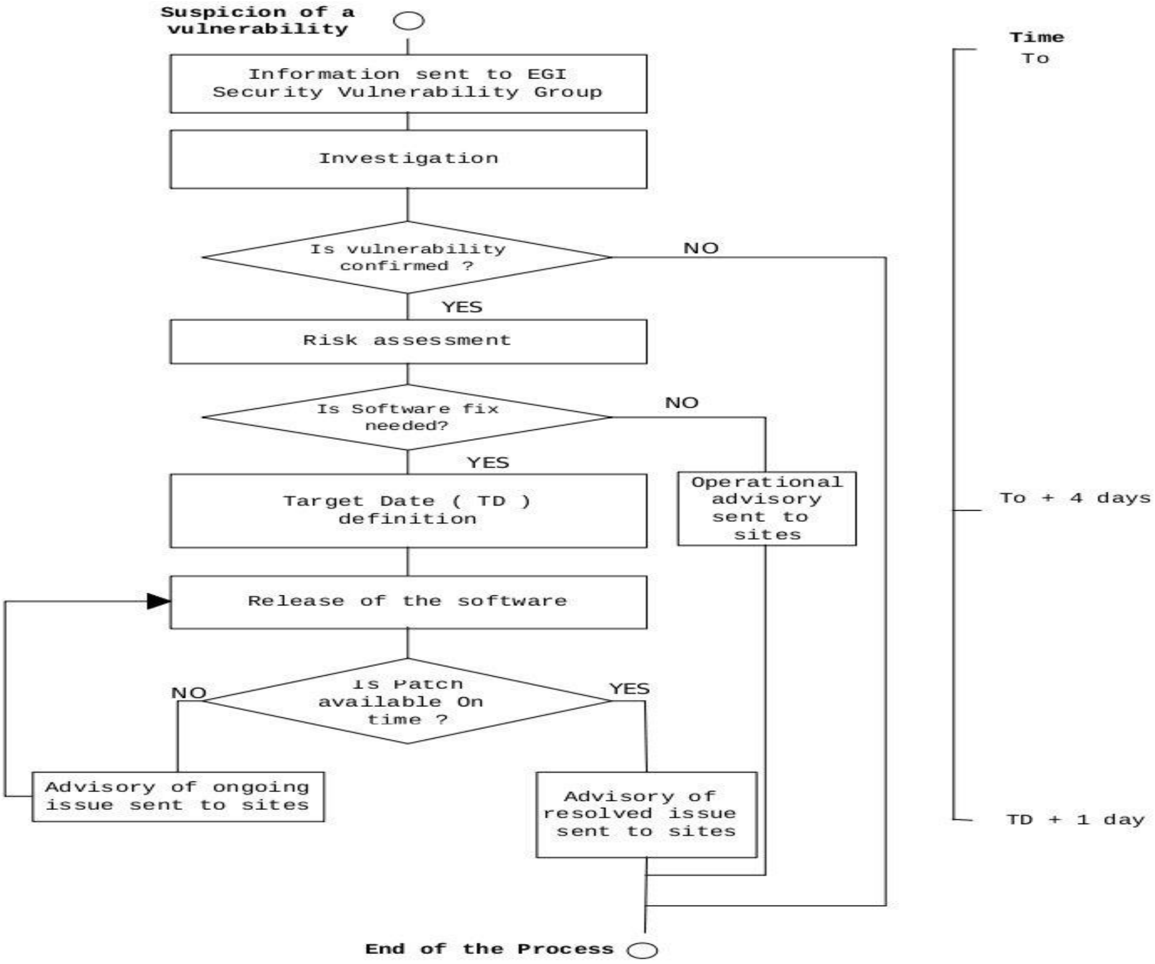
This procedure covers the handling of vulnerabilities reported to EGI. The risk posed by vulnerabilities in the EGI infrastructure needs to be first of all assessed; this allows the prioritization of the risk. It is primarily aimed at handling vulnerabilities in software available from UMD[2] repositories of EGI; but information reported on vulnerabilities in other software can be considered if the risk to the EGI infrastructure is important.

3.2 People involved

The overall process is the responsibility of the EGI SVG Risk Assessment Team (RAT).

Anyone may report vulnerability. The software providers are responsible for fixing a problem in time for the software to be released by the Target Date, and the EGI Deployed Middleware Support Unit is responsible for ensuring that software goes to production in time. In some cases EGI CSIRT may be asked to issue an advisory to mitigate a problem; if relevant, a critical vulnerability procedure[3] will then be raised.

3.3 Main steps


Suspicion of a vulnerability
Information sent to EGI Security Vulnerability Group
Investigation
Is vulnerability confirmed ?
NO
YES
Risk assessment
Is Software fix needed?
NO
YES
Target Date (TD) definition
Operational advisory sent to sites
Release of the software
NO
Is Patch available On time ?
YES
Advisory of ongoing issue sent to sites
Advisory of resolved issue sent to sites
End of the Process
Time
To
To + 4 days
TD + 1 day

[2] UMD - Unified Middleware Distribution – is the integrated set of software components contributed by technology providers and packaged for deployment as production-quality services in EGI.

[3] This procedure is described in section 4.

4 CRITICAL VULNERABILITY HANDLING

4.1 Purpose and scope

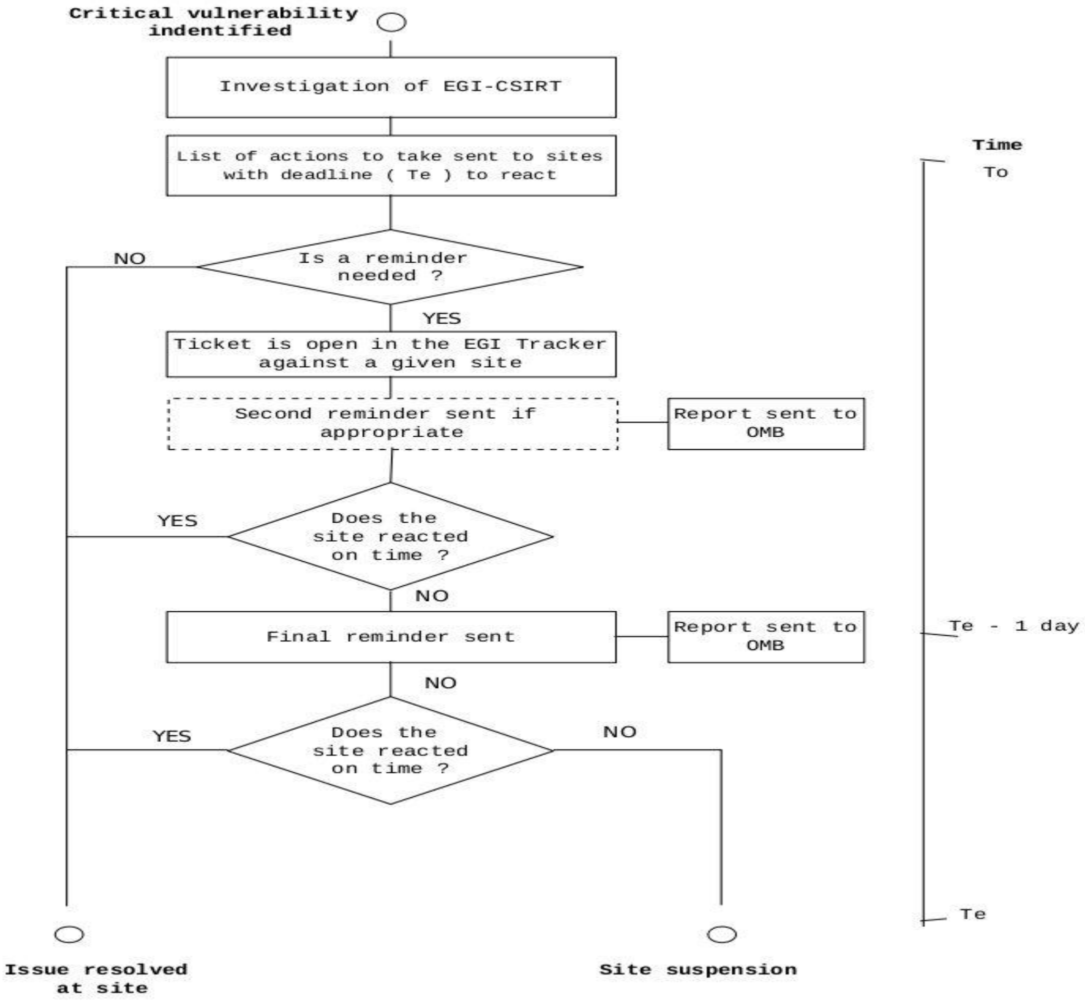
The aim of this procedure is to ensure that any critical security vulnerability is addressed in a timely manner. A critical security problem is one where it is considered that urgent actions need to be taken by sites. The most common case is likely to result from a software vulnerability assessed as critical, either in Grid Middleware or other software. Other critical vulnerabilities may occur, such as a configuration problem that the EGI CSIRT team assesses as critical. This procedure is also aimed to give sites adequate warnings before the suspension process is started and the site is removed from the EGI resource information system.

4.2 People involved

The overall process coordination is under the responsibility of EGI-CSIRT.

EGI-CSIRT investigates the problem and sends an advisory to sites. They also monitor the status of sites and start a suspension process if necessary. A majority decision of the OMB and/or the COO may overrule site suspension. At the NGI's level, NGI CSIRT should encourage their sites to take the recommended action. NGI-CSIRT also reports to EGI-CSIRT problems encountered by sites.

4.3 Main steps


Critical vulnerability indentified
Investigation of EGI-CSIRT
List of actions to take sent to sites with deadline (Te) to react
Time
To
Is a reminder needed ?
NO
YES
Ticket is open in the EGI Tracker against a given site
Second reminder sent if appropriate
Report sent to OMB
YES
Does the site reacted on time ?
NO
Final reminder sent
Report sent to OMB
Te - 1 day
NO
YES
Does the site reacted on time ?
NO
Te
Issue resolved at site
Site suspension

5 CONCLUSION

We saw that for security incident and vulnerabilities handling, roles and responsibilities are well defined.

EGI CSIRT coordinates incident handling and critical vulnerability handling procedures. And, EGI Security Vulnerability Group is in charge of the overall security vulnerability issue handling process. There is a strong collaboration between security teams and middleware providers. NGI CSIRT makes the link between sites within its NGI and EGI.

All these security teams working together with NGIs to achieve two key goals:

- Minimize the impact of a security incident,
- Reduce the likelihood of incidents by eliminating or mitigating software vulnerabilities.

Also, these operational security procedures are well documented and include definition of timescale and escalation steps. The approved releases of these procedures are available at: https://wiki.egi.eu/wiki/Operational_Procedures#Security.

6 REFERENCES

R 1	EGI.eu Policy Development Process https://documents.egi.eu/document/169
R 2	Security Policies within EGI https://documents.egi.eu/document/86
R 3	EGI CSIRT Term Of Reference https://documents.egi.eu/document/385
R 4	EGI SVG Term Of Reference https://documents.egi.eu/document/108
R 5	Working repository for Operational security procedures https://documents.egi.eu/document/693
R 6	Approved repository for Operational security procedures https://wiki.egi.eu/wiki/Operational_Procedures#Security
R 7	Non-operational security activities within EGI https://documents.egi.eu/document/307