EGI-InSPIRE

CSIRT Critical Security Operational Procedure

EU MILESTONE:NONE

Document identifier:	EGI-CSIRT-CriticalSecurity-V1
Date:	**15/12/2010**
Activity:	**SA1**
Lead Partner:	**EGI.eu**
Document Status:	**DRAFT**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/26

Abstract

This is a brief document describing the procedure for dealing with Critical Security Issues where action needs to be taken by a single site or multiple sites. Failure of sites to act on this or respond may lead to site suspension, as in such a situation the site is not considered secure enough to remain as part of the EGI infrastructure. Site suspension actually means removing the site from resource information systems. Approval from the OMB is sought for this procedure.

<<document handling and production procedure is provided in https://documents.egi.eu/document/33 >>

I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	The CSIRT Team		
Reviewed by	**Moderator:** **Reviewers:** <<To be completed by project office on submission to AMB/PMB>>		
Approved by	**AMB & PMB** <<To be completed by project office on submission to EC>>		

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	15th Dec 2010	First draft	
2			
3			

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

Overview

In order to prevent incidents, it is important to ensure that operational action is taken in a timely manner when a security problem has been found and a solution identified. A critical security problem is one where it is considered that urgent action needs to be taken, in order for both individual sites and the infrastructure as a whole to be secure. The most common type of critical security problem is where a software vulnerability has been found, and assessed as 'critical'.

After a problem has been assessed as critical, and a solution is available then sites are required to take action. This document primarily defines the procedure from this time, where sites are asked to take action, and what steps are taken if they do not respond or do not take action.

Definitions

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.

Intended Audience

This document is intended for grid site security contacts and site administrators in order to inform them what to expect and what is expected of them when they are asked to carry out an action to deal with a critical security problem. This document is also intended for Operations Management in order to give them visibility of the process, so that they may approve it.

Contact Points

Contact e-mail addresses used in this document:

site-security-contacts@mailman.egi.eu this address reaches the security contacts at all grid sites. The mailing list is automatically populated from GOCDB

ngi-security-contacts@mailman.egi.eu This is the National Grid Infrastructure security contacts list – again automatically populated from the GOCDB

noc-managers@mailman.egi.eu This is how to contact the National Operation Centre mangers.

manager-central-operator-on-duty@mailman.egi.eu Operators on duty – are able to suspend sites.

Chief operations officer – currently Tiziana Ferrari tiziana.ferrari@egi.eu

TABLE OF CONTENTS

1 INTRODUCTION

The procedure for handling of incidents by the EGI Computer Security Incident Response (CSIRT) is described in the EGI Incident handling procedure [R 1]. The procedure for handling software vulnerabilities (particularly in Grid Middleware which is part of the EGI UMD) by the EGI Software Vulnerability Group (SVG) is described in the Vulnerability issue handling process [R 2]. This is primarily about ensuring that the software available for installation in the EGI infrastructure is as free from vulnerabilities as possible. These two procedures have been approved together as Milestone MS405. However, a gap has been identified, in that after serious software vulnerabilities have been resolved it is important to ensure that all systems in the EGI infrastructure install an updated version of the software in a timely manner, and that any other serious operational security problem is resolved in a timely manner. This describes the procedure for ensuring that critical security issues are addressed in a timely manner and for giving sites adequate warning before removing from the EGI resource information system if they fail to make their sites secure.

The most common situation where critical security action needs to be taken is to install updates which resolve software vulnerabilities which have been assessed as 'critical' in the EGI environment. Critical vulnerabilities may occur in the Linux operating system, Grid Middleware provided from the EGI UMD, or other software. Of these the most common type of vulnerabilities to be assessed as critical are in the Linux operating system, as serious vulnerabilities in these are often made public and public exploits are available which is why they get assessed as critical. Usually the problem is widespread, affecting a large number of sites. Critical security problems may also be identified resulting from configuration problems, which may need action by sites.

The procedure is written to be agnostic relative to the systems used to establish site status, find information on sites, or track progress. This document focuses on affects on sites and CSIRT interaction with sites. Details of actual systems and what to do are maintained on the CSIRT private Wiki. More details of the procedure carried out by CSIRT including work carried out prior to establishing what action(s) should be taken by CSIRT is available in [R 3].

2 CSIRT ACTIONS AND RESPONSIBILITIES

Note that actions that fall out of hours are on a 'best efforts' basis. CSIRT actions may be carried out by the EGI CSIRT Security Officer on Duty, or by any member of the CSIRT team as agreed within the team.

2.1 Heads up issued

When a critical vulnerability has been identified, CSIRT may send a 'Heads Up' to sites. This is to inform sites of the problem and that urgent action may be requested in the coming hours or days.

This is OPTIONAL.

If sent, it SHOULD refer to any public information on the vulnerability, and why it is a problem in the EGI environment.

2.2 Find solution to problem

CSIRT MUST define what actions should be taken. This may be to install new versions of software which does not contain the vulnerability or make a configuration change that mitigates or removes the vulnerability. In exceptional circumstances when no solution is found in a reasonable timescale this may be to suspend or stop running certain software or services.

2.3 Send advisory with 7 day deadline

The EGI-CSIRT Security-Officer-On-Duty MUST send an advisory, this advisory MUST state what action is to be taken by sites in order to eliminate the critical security problem.

The covering letter MUST include the deadline for carrying out the action.

The deadline MUST be at least 7 days after the advisory is issued. If the deadline falls on a Friday, weekend, or common public holiday the deadline SHOULD be set to the first working day after allowing 7 days. It MUST also be clear that if sites do not carry out this action, and do not respond, then site suspension is a possibility.

It should be clear that CSIRT will help if necessary, and that if sites do not understand what to do or need any help they should contact CSIRT

For widespread problems, the letter and advisory MUST be sent to site-security-contacts@mailman.egi.eu and ngi-security-contacts@mailman.egi.eu and copied to noc-managers@mailman.egi.eu

For problems which only affect a small number of individual sites, the sites can be informed individually of the problem.

2.4 Allow 2 days for sites to act

Monitor the situation at various sites using appropriate tools.

After 2 days, for widespread problems if a large number of sites have not acted CSIRT SHOULD send a general reminder. This SHOULD include near the beginning "Thank you if you have already updated your site to fix the recent vulnerability" and include the advisory again.

2.5 After 3 days

For each site that is still vulnerable, after approximately 3 days, CSIRT MUST open a ticket in the EGI tracker. This MUST be sent to the site administrator, site security contact, and NGI security contact.

2.6 For each vulnerable site

Check daily whether the site has acted. If it has, CSIRT SHOULD close the ticket and include 'Thank you for addressing this problem'. If not, CSIRT MUST send a reminder.

2.7 24 hours before deadline

CSIRT SHOULD produce a list of which sites have not updated, and send this to noc-managers@mailman.egi.eu copying to the chief operations officer. This can be combined with the first step of the site suspension process as described in section 3.1

If all sites have updated, CSIRT SHOULD inform noc-managers, and there is no need for further action.

2.8 Respond to any requests communication with sites

CSIRT MUST respond to any request for more information or help from sites, and do all they can to help individual sites remove the critical security problem.

3 PROCEDURE FOR SITE SUSPENSION

In the case where sites fail to act on a critical security problem the site suspension procedure MAY be invoked at the discretion of CSIRT. The EGI Grid Site Operations Policy [R 4] allows sites to be suspended by removing the site from the resource information system. This procedure implements the policy.

Normally this procedure will be invoked AFTER the steps in section 2 to handle a critical security problem. In extreme circumstances (e.g. where an individual site has behaved in a reckless manner) it may be invoked independently.

3.1 24 hours before warning of site suspension

At least 24hours prior to starting the Suspension Procedure (i.e. before moving to the step described in section 3.2) CSIRT MUST send a summary to NGI-Management (noc-managers@mailman.egi.eu) with the following information:

- Which steps were taken by EGI-CSIRT.
- For each site which is still vulnerable
    - The name of the site
    - If the site has simply not responded, state this.
    - If the site has stated why the recommendations could not be followed, include this.
    - Include any relevant information on plans/alternative mitigation for the site.
    - Include whether CSIRT is recommending suspension for the site.
- State that if the situation does not change CSIRT plans to invoke the site suspension procedure.

3.2 Start the Site Suspension procedure

The EGI CSIRT MUST notify the affected site's security contact and NGI security officers that unless they carry out the recommended action by the deadline. The deadline MUST be at least 48 hours away, preferably 2 working days, and if this falls on a weekend or local public holiday the deadline SHOULD be on the following working day. Clearly state that failure to comply with the recommendations/advisories sent earlier might lead to site suspension.

It MUST be made clear that if there is a problem carrying out the recommended action CSIRT will try and help to find a solution. Attempts MUST be made to find a solution with the site if at all possible, and site suspension should only be invoked in the case of no response or failure to find a way to prevent it.

3.3 After 24 hours

If no acknowledgement from the site is received 24 hours before the site suspension deadline, CSIRT MUST send a further reminder to each site.

The NGI management at noc-managers@mailman.egi.eu and COO MUST also be informed of which sites continue to be vulnerable and their status, or if the critical security issue has been resolved for all sites.

3.4 On the Site suspension deadline

If EGI CSIRT takes the decision to suspend a site, the sites, CSIRT MUST inform NGI management (noc-managers@mailman.egi.eu) and COO about the decision including which sites are being suspended and why.

3.5 Request Site suspension

Ask the COD/ROD team to suspend the site(s); COD can be contact via: manager-central-operator-on-duty@mailman.egi.eu

4 SITES VIEW AND RESPONSIBILITIES

4.1 Site security is the responsibility of the site

Sites are responsible for their own security. CSIRT and other security groups in EGI exist to help keep sites secure. Sites MUST carry out some actions recommended by CSIRT in order for the site to remain part of the Grid, i.e. the site information being in the resource information system.

4.2 Sites will be informed of critical security problems, and given time to act

If a critical security problem has been identified, sites will be informed of what they need to do. Normally initially this will be general e-mail and advisory given to all sites

Sites SHOULD act to eliminate critical security problems as quickly as possible.

Sites MUST act before the deadline, which will be at least 7 days away.

If sites do not understand the advisory, or have a problem acting on it, sites SHOULD contact CSIRT for help.

4.3 Sites will receive at least 3 reminders before the site suspension is invoked

Sites may receive a general reminder 2 days after the initial advisory asking them to carry out appropriate action.

Sites will normally receive a reminder 3 days after the initial advisory and daily until the deadline, if they do not carry out the appropriate action.

4.4 Sites will get at least 48 hours notice of site suspension

This will give them another chance to act, and contact CSIRT if they need help. CSIRT will always attempt to find a solution for any site which cannot follow the instructions for some reason.

The combination of this and the initial minimum of 7 days means a site will only normally be suspended if they fail to act after 9 days.

5 NOC MANAGERS VIEW

5.1 NOC managers will be informed when action is requested to resolve a critical security problem

The notification and advisory, along with the deadline, will be copied to the NOC managers and the COO as in section 2.3

5.2 NOC managers will be informed of how many sites have not acted

Approx 24 hours before the deadline, NOC managers and the COO will be informed of how many sites have failed to carry out the requested action as in section 2.7

5.3 NOC managers will be informed 24 hours before the start of the site suspension procedure

NOC managers and the COO will be informed 24 hours before the site suspensions procedure is started. This will be as stated in section 3.1 and may be combined with the information received in 5.2

5.4 NOC managers will be informed prior to site suspension

NOC managers and the COO will be informed before CSIRT actually suspends sites due to non-compliance with the 48 hour warning as in section 3.4.

5.5 NOC managers will be informed when all sites have acted

NOC managers and the COO will be informed when all sites have acted to resolve a critical security problem.

6 REFERENCES

R 1	The EGI Security incident handling procedure MS405 https://documents.egi.eu/public/ShowDocument?docid=47
R 2	The EGI Software Vulnerability Issue handling process MS405 https://documents.egi.eu/public/ShowDocument?docid=47
R 3	The EGI Critical Vulnerability Handling procedure https:// documents.egi.eu/public/ShowDocument?docid=282
R 4	EGI Grid Site Operations Policy https://documents.egi.eu/secure/ShowDocument?docid=75
R 5	