EGI.eu

EGI Federated Cloud Security Questionnaire for Technology Providers

Document identifier	EGI SVG checks for technology providers
Document Link	https://documents.egi.eu/document/<DOCID>
Last Modified	23/07/2014
Version	0.7
Policy Group Acronym	SVG
Policy Group Name	EGI Software Vulnerability Group
Contact Person	Linda Cornwall, Sven Gabriel, Maarten Litmaath
Document Type	Procedure/Questionnaire
Document Status	DRAFT
Approved by	EGI OMB?
Approved Date	DD/MM/YYYY

Policy Statement

This is a questionnaire/procedure which allows for a basic understanding of the manner in which a technology enabling cloud services works from a security point of view. It allows an assessment that the cloud enabling technology is sufficiently secure for the EGI security teams to recommend it is used in the EGI infrastructure.

I. AUTHORS LIST

	Name	Partner/Activity/ Organisation/Function	Date
From	SVG/CSIRT		

II. DELIVERY SLIP

	Body	Date
Reviewed by	TCB	DD/MM/YYYY
Reviewed by	OMB	DD/MM/YYYY
Reviewed by	UCB	DD/MM/YYYY
Approved by	EGI.eu Director	DD/MM/YYYY
Approved by	EGI.eu Executive Board	DD/MM/YYYY

III. DOCUMENT LOG

Version	Date	Comment	Author/Organization
0.1	14th Feb 2014	First draft for discussion, based on e-mail exchanges.	Linda Cornwall/STFC

0.2	24th Feb 2014	Small changes – better explanation of maintenance/security support	Linda Cornwall
0.3	25th Feb 2014	Modifications after comments by Oxana Smirnova and Stephen Burke	Linda Cornwall
0.4	26th Feb 2014	Modifications after comments by Maarten Litmaath, Sven Gabriel	Linda Cornwall
0.5	5th March 2014	Addressed comments from Paul Millar, Alvaro Lopez Garcia	Linda Cornwall
0.6	31st March 2014	Addressed comments by Sven Gabriel	Linda Cornwall
0.7	23rd July 2014	Added clarification and more questions on vulnerability handling, plus questions on context of person filling in.	Linda Cornwall
1.0			
2.0			
3.0			
4.0			

IV. APPLICATION AREA

This document is a formal EGI.eu policy or procedure applicable to all participants and associate participants, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

V. POLICY/PROCEDURE AMENDMENT PROCEDURE

Reviews and amendments should be done in accordance with the EGI.eu "Policy Development Process" (https://documents.egi.eu/document/169).

VI. ORGANISATION SUMMARY

To support science and innovation, a lasting operational model for e-Infrastructure is needed − both for coordinating the infrastructure and for delivering integrated services that cross national borders. The objective of EGI.eu (a foundation established under Dutch law) is to create and maintain a pan-European Grid Infrastructure in collaboration with National Grid Initiatives (NGIs) in order to guarantee the long-term availability of a generic e-infrastructure for all European research communities and their international collaborators.

In its role of coordinating grid activities between European NGIs, EGI.eu will:

- Operate a secure integrated production grid infrastructure that seamlessly federates resources from providers around Europe
- Coordinate the support of the research communities using the European infrastructure coordinated by EGI.eu
- Work with software providers within Europe and worldwide to provide high-quality innovative software solutions that deliver the capability required by our user communities

- Ensure the development of EGI.eu through the coordination and participation in collaborative research projects that bring innovation to European Distributed Computing Infrastructures (DCIs)

The EGI.eu is supporting ‘grids’ of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI.eu will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop grids, to benefit the user communities within the European Research Area.

EGI will collect user requirements and provide support for the current and emerging user communities. 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 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, 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 − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

TABLE OF CONTENTS

1 INTRODUCTION

The EGI infrastructure has been based on Grid Technology for more than a decade, and the Grid based technology is very mature from a security point of view. Now that new technology (primarily cloud technology) is being deployed it is important to ensure that this technology is as secure as possible.

The main aim of this document is to provide a list of checks and considerations in the form of a questionnaire for cloud enabling technology providers. This will allow an understanding of how the technology works from a security point of view, whether it is able to comply with the EGI policies in particular concerning User/Identity handling, User/Identity suspension, logging and traceability. It allows the EGI security teams to assess whether this technology is suitable for inclusion in the EGI infrastructure.

This questionnaire needs to be filled in for any technology which is deployed on the EGI infrastructure. This provides some assurance that at least at the time this questionnaire is filled in, it does not contradict EGI security policy. It is not a CSIRT responsibility to fill in the questionnaire. The questionnaire may be filled in by one of the following:

- By the technology providers developing the software (for example if the technology is produced by a collaborating project)
- By an individual within EGI who takes the role to be the contact to the technology providers. (This person would also take the role as the contact in case of vulnerabilities.)
- EGI sites deploying a certain cloud technology. (If more than one site is using a certain product it might make sense to coordinate the activity answering the questionnaire.)
- By anyone with a relationship with EGI with expertise on this particular technology.

This is not a detailed vulnerability assessment, and does not guarantee that the software is secure. It also does not guarantee that the technology provider does not change the software in a way which no longer satisfies the security requirements of the EGI infrastructure. The person filling out the questionnaire is trusted to be honest.

In order to be able to address security problems that may be found at a later date, it is important that the software is under security support, and that if we contact the technology provider then we can expect a response and reported security problems to be fixed.

2 PERSON OR PERSONS FILLING IN THE QUESTIONNAIRE

2.1 *Name and Contact details*

Name and e-mail address.

2.2 *Name of the technology you are answering questions on*

Please state the name of the technology you are answering questions on.

2.3 *Are you a member of the product team?*

Please state whether or not you are a member of the product team.

2.4 *If you are not member of the product team, state the context in which you are filling out the questionnaire.*

Examples may include that you have a close relationship with this product team, or you have expertise with this product, or you plan to deploy this product, or anything else.

3 DESCRIPTION OF THE PRODUCT FEATURES

This is intended to provide a basic functional understanding of the product from a security point of view. Short answers are preferred. Existing documentation may be referred to in order to help answer these questions.

3.1 *Please provide and/or refer to existing documentation*

Please supply existing documentation. You may forward electronic copies, or provide a link if it is available online.

3.2 *Describe all components of the system.*

Describe in a schematic way all components of the system. If a component needs to use IPC to talk to another component for any reason, describe what kind of authentication, authorization, integrity and/or privacy mechanisms are in place. If configurable, specify the typical, minimum and maximum protection you can get. This in particular may be a reference to an already existing document. A reference to an existing Architectural Design Document or something equivalent would be an appropriate answer.

3.3 *Identity technology used*

Define or describe what technology or technologies are used by the product to identify users. You may refer to any open standard which defines the technology.

3.4 *User identity handling*

Describe how user identities are handled by the system in all places where they are used. This includes querying the system, launching a task, access to storage, creating a network, deleting a machine etc. This credential handling should be described from the moment a user submits work to the system to the moment that a task runs, through any intermediate storage of credentials.

3.5 *Identity management and changes*

If the user identity changes in any way, e.g. a task is carried out under a different identity from that of the original user identity; describe what happens around identity changes. Describe how actions are attributed to the original user. (An example may be if a generic or shared identity is used to access a database.) The answer to this may be 'none' if that is the case.

3.6 *Can an individual user identity be blocked?*

It is an EGI policy requirement that identities can be blocked from accessing EGI resources.

Is this functionality implemented in this technology?

Briefly describe how it is supposed to work.

EGI policies defining this requirement include The EGI Security Policy [R 5] section 2.5.4, and The EGI Service Operations Security Policy [R 6] statement 9 where it is stated "You must implement automated procedures to download the security emergency suspension lists defined centrally by Security Operations and should take appropriate actions based on these lists, to be effective within the specified time period.

3.7 Describe how a user task is created

Describe how a user task is created and how it is destroyed. If your service has long-running activity (e.g. more than 24 hours) associated with a user, describe the life-cycle of this activity.

3.8 Describe how each user and task is isolated.

Describe how each user and each task is isolated from others. How does the software prevent users accessing or interfering with other user's tasks or VMs?

3.9 Describe how actions of a user are logged

Describe how actions of a user are logged, how they can be attributed to the correct user identity.

State whether it is possible to archive logs. Include whether this may achieved in a manner in which the user cannot tamper with logs, in particular concerning actions such as connections outside the VM.

4 QUESTIONS ON CODE

This describes some basic questions on the code. Suitable answers reduce the likelihood of some common software vulnerability types and also allow the code to be maintained if vulnerabilities are found at a later date.

4.1 *Software licence*

Please state the software licence.

Please also indicate whether the software is an Open Source Initiative approved licence [R 4].

4.2 *Has any sort of assessment been made by security experts on the software?*

If any security testing or security (vulnerability) assessment has been carried out on the software please forward any reports you have. If the answer is no, then this is not a problem. It is useful for us to know what level of security assessment has been made on each product. If the product has already been examined by recognised security experts then this will give us confidence in the product.

4.3 *Is user input sanitized?*

Are steps taken in order to attempt to sanitize or validate all user input?

Many types of vulnerability come from the failure to validate user input, allowing users to induce the software to behave in a way that was not intended. These include buffer overflow vulnerabilities, SQL injection vulnerabilities, among others.

It is not sufficient to only accept input from a trusted client, as clients external to a Cloud Resource Provider may be modified.

It is necessary to confirm that all user input has undergone some sort of validation or sanitation, including that from external clients which are supplied with the product as they may be modified to produce malicious input. It is not expected to guarantee there are no bugs or problems with the validation process, just that there is some attempt to validate input.

4.4 *Check file permissions*

Many software vulnerabilities come from file permission errors, e.g. an executable with world write permission may allow a user to overwrite it, or a configuration file containing sensitive information which others can read. Check that on an installation of the product (e.g. newly installed, default configuration) that there are no obvious file permissions which are likely to cause security problems.

5 CONTACT DETAILS AND MAINTENANCE

It is important that if a security problem is found with the software that it is possible to contact the software provider, and that any vulnerability is investigated and fixed in a timely manner.

The majority of the Grid technology software was provided by EMI (and it's successors) and Globus. EGI has had a Service Level Agreement with these organisations which includes vulnerability handling, and EGI continues to have a strong working relationship with these groups and development teams. The EGI SVG has been the main way in which software vulnerabilities are reported in the software, in particular for EMI software. I.e. most vulnerabilities have been reported to EGI, and then handled by the EGI vulnerability issue handling procedure.

Software such as the Linux operating system is maintained by the software providers, and they handle vulnerabilities themselves and announce any problems when they are fixed. EGI is not in any Service Level Agreement with these, but vulnerability handling happens in a suitable way. One example is RedHat who provide a suitable procedure for handling vulnerabilities [R 3]. The majority of vulnerabilities in this case are reported by others, outside EGI, and it is for the EGI security teams to decide on the relevance and risk to the EGI infrastructure usually after they have been announced as fixed. Only for the more critical vulnerabilities has EGI had to take any action in this case.

For both these types cases EGI has not had problems with known vulnerabilities remaining in the software and being unable to get them fixed, in both these cases vulnerabilities are handled in a suitable manner. For some other software deployed it has been difficult, if not impossible to get vulnerabilities fixed, and this is what we want to avoid.

5.1 Please confirm that this software is under security support.

Please confirm that this software is under security support. This means that if security problems are found they will be investigated and fixed where necessary.

5.2 Please state how long this software is going to be under security support

This can be in the form of a link to a security support policy, in the case of a large commercial supplier, or a simple statement from a smaller supplier.

5.3 Please state how software security problems are to be reported

It is important to be able to report any software vulnerabilities found to a technology provider.

This may be an e-mail contact. Note that it is better that more than 1 security contact is provided, or the security contact is in the form of a mail list which goes to more than one person on the product team. In case a serious problem is found where one person is not available.

This may be a link to a security maintenance page or ticketing system.

5.4 Confirm that it is possible to report a problem to the security team without creating a public ticket or e-mail with a public archive

Confirm that you have checked (either with the provider, or from your own expertise) that it is possible to report a problem, information goes to the security team, without the information being made public. For larger commercial providers checking that e.g. a support form includes the option of creating a private ticket. An e-mail to a list which does not contain a public archive is also a sufficient check.

5.5 Does the Technology Provider have its own vulnerability handling function and/or policy?

Most of the larger technology providers will have a team and strategy for handling vulnerabilities, for investigating and assessing. If so, please provide a link or information on this.

For smaller/collaborative providers, they may not have a vulnerability handling activity. In this case they may wish their vulnerabilities to be handled by the EGI procedure.

5.6 Does the technology provider announce vulnerabilities?

Many of the larger providers announce fixes to vulnerabilities found. Does this provider have a system for announcing when vulnerabilities are fixed? If so, please provide a link and/or information.

5.7 Does the technology agree to collaborate with EGI software vulnerability handling?

This is only relevant if you are either a member of the product team, or have a relationship with the product team. For larger commercial suppliers we do not ask for any agreement, provided they have a satisfactory vulnerability handling procedure in 5.5.

In the EGI infrastructure, software vulnerabilities are handled by the EGI Software Vulnerability Group (SVG) according to the approved EGI Software Vulnerability issue handling procedure [R 1]. This is important because we do not wish to find some software is deployed widely in the EGI infrastructure, a security vulnerability is found, yet we cannot get it fixed.

Basically this means that if a potential software vulnerability is reported to us you agree to investigate it, co-operate with the EGI SVG, and if it is valid fix it in a timely manner. A simple summary of the procedure is available on the Wiki at [R 2]. A member of your product team may join the EGI Software Vulnerability Group (SVG) Risk assessment team if you wish.

6 ANY OTHER INFORMATION

Provide any other information you wish. (Optional.)

7 POTENTIAL OUTCOMES AND CONCLUSIONS

7.1 *Result of the Assessment*

Likely outcomes after the EGI security groups have looked at the Technical providers response are one of the following:

- Request for more information/ information in a different form.
- This is well thought out and it perfectly fits in existing user management used in grid infrastructures.
- To integrate in existing user management in grid infrastructures, please do this ….
- This is incompatible with user management in the EGI Infrastructure, we cannot support it as it is.

8 REFERENCES

R 1	EGI Software Vulnerability Issue Handling procedure https://documents.egi.eu/secure/ShowDocument?docid=717
R 2	https://wiki.egi.eu/wiki/SVG:Issue_Handling_Summary
R 3	Red hat vulnerability handling https://access.redhat.com/site/security/team/contact/
R 4	Open Source Licences http://opensource.org/licenses
R 5	Grid Security Policy https://documents.egi.eu/public/ShowDocument?docid=86
R 6	Service Operations Security Policy https://documents.egi.eu/public/ShowDocument?docid=1475