EGI-InSPIRE

The Software Vulnerability Issue handling process

EU DELIVERABLE: MS405-SVG

Document identifier:	EGI-MS405-SVG-V8.doc
Date:	**03/08/2010**
Activity:	**SA1**
Lead Partner:	CNRS for Deliverable/STFC for SVG
Document Status:	**Draft**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/47

Abstract

In order to reduce the risk of computer security incidents, it is important to handle and resolve software vulnerabilities reported in the EGI infrastructure. This document describes the process for Grid Software Vulnerability Issue handling by the EGI InSPIRE project. It describes what is meant by a vulnerability, how to report a vulnerability, and how vulnerabilities are handled. It describes the responsibilities of various people within the Software Vulnerability Group (SVG), the EGI InSPIRE project and in the communities providing software distributed in the EGI Unified Middleware Distribution and how the various groups interact with this process.

Delivery Slip

	Name	Partner/Activity	Date
From			
Reviewed by	**Moderator:** Sergio Andreozzi **Reviewers:** Dr Josva Kleist	NDGF	14th July 2010
Approved by	**AMB & PMB**		

Document Log

Issue	Date	Comment	Author/Partner
1.0	25/06/2010	First draft	STFC/Dr Linda Cornwall
2.0	01/07/2010	Second draft – after comments from SVG (Maarten Litmaath and Mischa Salle) and Leif Nixon	STFC/Dr Linda Cornwall
3.0	02/07/2010	3rd Draft - after comments from Dorine Fouossong and further comments from Maarten.	STFC/Dr Linda Cornwall
4.0	02/07/2010	Changed data format to dd/mm/yyyy	STFC/Mingchao Ma
5.0	05/07/2010	Changed ToC to display level 2; Minor format update	STFC/Mingchao Ma
6.0	05/07/2010	Minor format update	STFC/Mingchao Ma
7.0	19/07/2010	Addressed reviewers comments (Dr Josva Kliest)	STFC/Dr Linda Cornwall
8.0	03/08/2010	Addressed Tiziana Ferrari comments.	STFC/Dr Linda Cornwall

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 the 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 the ESFRI projects. 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 – 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

1.1. Purpose

The purpose of this document is to describe the EGI Software Vulnerabilities Group (SVG) and the process for handling software vulnerabilities found in the EGI infrastructure.

1.2. 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.

This document is relevant to anyone who interacts with the EGI infrastructure, in that it informs how to report a vulnerability and how each vulnerability is dealt with. It is particularly relevant to those who provide the Grid Middleware used in the EGI infrastructure, contribute resources to the EGI infrastructure, or distribute software for the EGI.

1.3. References

Table 1: Table of references

R 1	The (EGEE) Grid Security Vulnerability Group – Process and Risk Assessments for Specific Issues https://edms.cern.ch/document/977396
R 2	The EGI InSPIRE Incident Response Procedure https://documents.egi.eu/secure/ShowDocument?docid=47

1.4. 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

This document will be revised as the project proceeds, and further information and documents become available.

1.5. Terminology

A complete project glossary is provided in the EGI-InSPIRE glossary:
http://www.egi.eu/results/glossary/

Glossary

CSIRT	(The EGI) Computer Security Incident Response Team
EGEE	The EU Enabling Grids for EscienceE project
GSVG	(The EGEE) Grid Security Vulnerability Group
IRTF	The (EGI) Incident Response Task Force
NGI	National Grid Infrastructure

RAT	The Risk Assessment Team
SVG	(The EGI) Software Vulnerability Group
TBC	To Be Confirmed
TBD	To Be Determined
TD	Target Date
UMD	(The EGI) Unified Middleware Distribution

2. EXECUTIVE SUMMARY

To ensure the sustainability of the deployed EGI infrastructure it is important that it is sufficiently secure. The main purpose of security is to allow people to enjoy the benefits they are entitled to. If the infrastructure is not secure, for example if users' data is destroyed or exposed, or users cannot use the system because it has been damaged then users will demand other means of carrying out their activities. If incidents happen where sites are compromised then sites will not with to participate and provide resources to the grid.

A large part of ensuring that the infrastructure is secure is to ensure that the software deployed is secure, by eliminating existing software vulnerabilities and preventing the introduction of new ones. This is the task of the EGI Software Vulnerability Group. This document describes how software vulnerabilities found or reported are handled.

The basic process is that:

- Anyone may report a vulnerability by e-mail to report-vulnerability@egi.eu
- The Risk Assessment Team, along with the reporter and developer investigate the issue, to see if it is valid.
- If a reported issue is found to be valid, the Risk Assessment Team place the issue in one of four risk categories – Critical, High, Moderate, or Low.
- According to the risk category, a fixed target date for fixing this vulnerability is set.
- The developers then should try and fix the issue by the target date.
- An advisory is released when a fixed version of the software is released, or on the target date, whichever is the sooner.

This document describes this process in more detail, and defines the responsibilities from the point of view of the various parties involved, i.e. the Reporter of the Issue, The Software Vulnerability Group, The Software providers, the EGI Middleware Unit, Security Operations and the sites.

3. Scope of the SVG issue handling activity

3.1. Background

In 2005 it was recognised that something should be done to log and try to fix/eliminate vulnerabilities in the grid infrastructure in order to reduce the likelihood of incidents. The Grid Security Vulnerability Group (GSVG) was included in the EGEE-II proposal. A process for handling vulnerabilities, setting a target date for fixing the issue, and responsible disclosure was established and approved by the EGEE management for software produced by EGEE [R 1]. Such an activity is also recognized as being necessary for software used in the EGI infrastructure, and the EGI Software Vulnerabilities Group (SVG) was included in the EGI proposal.

3.2. Changed Situation for EGI

For the EGEE GSVG, the focus was very much on software provided as part of gLite. Permissions for releasing information on vulnerabilities according to the agreed process were only admissible for gLite, as it was part of the EGEE project. For EGI, the situation is different. The EGI InSPIRE project is distributing software provided by 3rd parties, by the EGI Middleware Unit as part of the EGI Unified Middleware Distribution (UMD). A service level agreement between EGI and the software providers is being defined which gives the SVG permission to handle vulnerabilities according to the agreed process, and which has the software providers agree to a response time if a potential vulnerability is found in the software they supply.

Some other changes to the process are being made. The amount of time allowed to fix vulnerabilities after the assessments are complete has been lengthened (TBC), partly to allow a more realistic schedule for all but the most critical issues, and partly because in EGEE the timescales were probably set much stricter than needed.

3.3. Scope of SVG

Between EGI Computer Security Incident Response Team (CSIRT) and EGI SVG all problems concerning security of the deployed EGI infrastructure should be dealt with. It is worth noting that sites are responsible for their own security, CSIRT will advise and recommend on security matters and have the power to suspend sites from the infrastructure if they fail to apply critical security patches.

The handling of incidents is the responsibility of the EGI Incident Response Task Force (IRTF) and they are handled according to the Incident Response Procedure [R 2]. However, if an incident turns out to be due to a software vulnerability then the SVG may get involved. SVG should ensure that the software available for installation on the EGI infrastructure is sufficiently secure and contains as few vulnerabilities as possible, thus reducing the likelihood of incidents. In particular SVG handles vulnerabilities reported in the software distributed by EGI (in the UMD) in the manner described in this document and defined in section 3.5. Vulnerabilities in 3rd party software distributed in the UMD including dependencies for which there is a patch from the provider may also need to be partially handled by SVG. If either a dependency is re-distributed in the EGI UMD, or if it is necessary to ensure that the software which is dependent on it works with a new version, then SVG may need to be involved. The risk posed by the vulnerability in the EGI infrastructure needs to be assessed by SVG to establish the timescale for which the EGI UMD should include the fixed dependency.

SVG may also handle other software vulnerabilities in software used in the EGI infrastructure, as appropriate.

SVG will not normally be involved for vulnerabilities in operating systems, as appropriate patches are usually issued by the vendors of those systems, and advisories are issued as well. It is then an operational (CSIRT) activity to decide on the priority of upgrading such software. However, SVG can be consulted by CSIRT, on general vulnerabilities and other matters where appropriate.

3.4. Scope of this Document

This document describes how specific potential vulnerability issues reported to or found by the EGI Software Vulnerability Group are handled. It describes the interfaces between the various groups involved in handling issues. It does not cover other activities, such as checking code and assessing software for vulnerabilities, ensuring new code introduced into the EGI infrastructure is secure, or developer education. It does include the handling of vulnerabilities found as a result of assessing software for security, which are handled in the same way as vulnerabilities found or reported in other ways.

3.5. What is a vulnerability

We usually consider a vulnerability as a problem where a principal can gain access or influence a system beyond their intended rights. This could be where an unauthorized user may gain access to a system. This could be where a user gains privileges they should not be able to hold, such as root or administrator privilege, can damage a system, gain access to data or information that is confidential, or impersonate another user. It can also be if a user is able to cause damage to a 3rd party via usage of the system.

Some people who carry out vulnerability assessments do not report issues if they cannot develop an exploit. SVG does require a proof of concept piece of software to be developed in order for a problem to be treated as vulnerability. Dangerous coding constructs, where there is a possibility that an exploit can be developed, can be considered to be vulnerabilities. However, if the risk is considered to be negligible then the issue may be treated in another way, e.g. as a bug, as the people assessing the issue considers appropriate.

3.6. What is NOT a vulnerability

3.6.1. Actions that can only be carried out by site administrators

In general, site administrators are (almost) trusted at the sites they manage – and they are assumed to be able to access and manipulate data stored on their equipment. The only thing that they are not trusted with is bulk encrypted data and encryption keys. Site administrators should not be able to decrypt encrypted data at will, however as data needs to be decrypted for processing it cannot be entirely protected from processes with site administrator privileges.

3.6.2. Issues which provide information that may be useful to an attacker

If information is provided which may be of use to an attacker, but does not represent an exploit in itself, this is not necessarily considered to be a vulnerability. In the past such issues have been treated as ‘Low’ risk issues, even if there is virtually no risk. These can again be rejected, treated as standard bugs or as vulnerabilities as the RAT considers appropriate.

3.6.3. General Concerns

This is the type of report where someone states that ‘this may not get installed correctly’ or ‘some users will do this incorrectly’. Such concerns will not be considered vulnerabilities, but can be raised with the appropriate groups. If they are reported to SVG then SVG will raise them to the appropriate groups.

4. Issue handling process

4.1. The Risk Assessment Team (RAT)

The Risk Assessment Team (RAT) is the group of people within the Software Vulnerability Group (SVG) who carry out the issue handling process of the SVG, and are party to information on vulnerabilities which have not been disclosed publically. As the phrase Risk Assessment Team implies, one of their main duties is to assess the risk associated with a software vulnerability found, so that a software vulnerability can be fixed in a timely manner according to the severity of the problem.

The RAT members include developers from the various software provider teams whose software is included in the EGI UMD, NGIs and experienced site administrators.

Some members of the RAT (in particular the chair of the activity) also co-ordinate the activity to ensure that the process is carried out as stated in this document. These are members of the EGI project. This includes making sure that contact details for the developers are in available the infrastructure is in place, and the various parts of the process are carried out in a timely manner.

4.2. Basic process

4.2.1. Reporting an issue

If anyone finds a suspected vulnerability, they should report it to

report-vulnerability@egi.eu

It is then entered into the Software Vulnerability Issue tracker. This is a private tracker, information can only be accessed by the RAT and others involved in the fixing of the issue.

4.2.2. Investigation of issue

It is then investigated by the RAT in conjunction with the reporter of the issue and the supplier of the software. The RAT is the group of people who are party to information on vulnerabilities which have not been disclosed and carry out most of the issue handling work. This is in order to establish whether or not there is an issue, and if there is what the problem is, in what circumstances it may be exploited and what the probable effect of exploitation is.

If as a result of this investigation it is agreed that no problem exists then no further action is taken.

4.2.3. Risk Assessment

Assuming a problem exists a risk assessment is carried out by the RAT which discusses the impact of each issue. The RAT then places the issue in one of 4 risk categories:

- Critical
- High
- Moderate
- Low

The category is established by vote, i.e. the RAT members vote in which risk category an issue should be placed. Usually a clear majority of the votes are for a particular risk category, which is then taken as the resulting risk category. When the votes remain divided after ample discussion, either the more conservative (i.e. higher) level is taken, or the matter may end up deemed out of scope for the SVG, as explained in section 3.6. In some such cases the CSIRT may be asked to consider an operational advisory. In others it may be concluded that there is no vulnerability, and the RAT and the software provider may consider whether other action needs to be carried out, such as submission of a standard bug.

4.2.4. Target Date Set

A Target Date (TD) for fixing is set according to the risk category, as below.

(TBD and debate encouraged – For EGEE dates were 2 days, 3 weeks, 3 months, 6 months – suggest revise upwards definitely not downwards.)

- Critical – 3 days (see section 4.3)
- High – 6 weeks
- Moderate – 4 months
- Low – 1 year

This is from the day that the risk category is set. The reason for this is to allow the prioritization according to severity and timely fixing of vulnerabilities in the software.

The software providers, UMD, and reporter are informed of the risk category, and of the target date for fixing the issue.

The SVG aims to reach this point, i.e. where the risk category is set, within at most 4 working days of an issue being reported. Usually this should be done within 2-4 working days, which is a realistic aim to allow time to contact the RAT and the developers, investigate the problem, find the likely impact if the issue were to be exploited and assess the risk. This may be done more quickly in the case of issues assessed as critical, see section 4.3

.

4.2.5. Fixing the issue

It is then between the software providers and the EMI middleware unit arranging the distribution of the software to try and ensure that the issue is fixed by the target date, and the version of the software available in the UMD on the target date for installation across the EGI infrastructure does not contain the vulnerability.

4.2.6. When the issue is resolved

When the new version of the software is released, i.e. made available in the UMD, with the issue resolved an advisory is issued by the SVG. The release notes should refer to the advisory, and the advisory should refer to the release notes.

4.2.7. If the target date is reached and no patch is available

The advisory is released on the target date, or the first working day after the target date. This may not necessarily be the case for Critical issues, see section 4.3.

4.3. Special process for critical issues

It is usually apparent quite quickly if an issue falls into one of the higher risk categories, and investigation tends to happen quickly. Hence in this case the aim is to investigate the issue and assess the risk within 1 working day. It is probably more important to simply establish whether the problem is real and find a short term solution, than carry out a full investigation and decide on a long term solution.

While it is hoped that none of these occur, or if they do it will be rare, it should be noted that if a critical issue does occur a special process will need to be carried out. What should be done will need to be considered on a case by case basis.

This will include:

- Alerting CSIRT, developers, and the EGI middleware unit as soon as a possible Critical issue has been identified.
- Consider whether it is practical to make fix the software and make a release on a very short time scale. This will involve a discussion with the developers and the EGI middleware unit.

- If it is not, then in conjunction with CSIRT, developers, reporter and any other appropriate people discuss what should be done in the short term. This may be to advise sites to disable a service until the problem can be resolved, or take some sort of other mitigating operational action. This will need to be considered on a case by case basis.
- Another option may be to set a longer target date than the default 3 days, but this should be agreed between the software providers, SVG, and CSIRT.
- Inform sites on what should be done. This may be in the form of a normal advisory, or it may require special action.

4.4. Issuing advisories

Advisories are issued publicly on the web at
http://www.gridpp.ac.uk/gsvg/advisories/

This will probably move to an EGI Wiki –

This will probably continue to be publicly readable, but the possibility of making it readable only by those who can logon to EGI using an EGI SSO account will be considered.

The EGI CSIRT Team, sites, along with the reporter of the issue will then be informed of the availability of the new advisory. The exact lists which will be used to inform sites and possibly others are not certain yet.

Advisories should include the type of problem that would occur if the vulnerability were to be exploited, but not include how to exploit the vulnerability.

4.5. Principles of dealing with other situations

While the majority of issues are expected to result from bugs in the software included in the UMD, a minority of issues are likely to fall into the outlined categories below.

4.5.1. Operational Vulnerabilities

Some issues may turn out to be purely operational, and no software fix is required. In this case CSIRT is informed of the problem with any appropriate recommendations.

4.5.2. Issues where the decision is not to fix

This may be because there isn't a practical way of fixing it, or the problem is part of the design of the system. In this case CSIRT will be informed, with recommendation of any mitigating action that should be taken or problems they should be alert to.

4.5.3. Other cases

The principle is that any issue where there is an exploitable vulnerability should be dealt with in some way, but not in a way that provides information publicly that is useful to a potential attacker.

5. Reporters view and responsibilities

5.1. Not publicising a vulnerability

It is important that information on vulnerabilities is kept private while they are investigated and while the software providers are fixing them. Vulnerabilities must not be entered on any publicly readable bug tracking system, discussed on any mailing list that is either publicly archived or does not have a strictly controlled membership policy, or placed on any web page.

Vulnerabilities should not be publicised in any way without agreement from the SVG.

If a vulnerability has been distributed publicly, e.g. on a less secure mailing list, or on a publicly accessible web page, then the reporter should make this known to the SVG and if possible try to ensure the information is removed.

5.2. Reporting a vulnerability

Anyone who finds a vulnerability should report it to the EGI SVG via report-vulnerability@egi.eu

5.3. Help and co-operate with the investigation

While this is not mandatory, it is can be extremely helpful if the person who finds a vulnerability is able to assist with the investigation.

5.4. Reporter receives information

The reporter will receive information on the outcome and conclusion of the investigation, including the risk category and Target Date, and will receive a copy of the advisory.

6. Software Vulnerability Group (SVG) view and responsibilities

6.1. Set up and maintain infrastructure for issue handling

The Software Vulnerability Group (SVG) will set up and provide the infrastructure for issue handling. This includes the mailing list for reporting, the mailing list for the RAT to investigate and assess issues, and the web pages for release of advisories. It also involves ensuring that the contact details for the various software providers are at hand and readily available.

6.2. Provide a rota for cover on working days

SVG will try and ensure that a person is available to respond to any issue reported and carry out the issue handling process on all working days. This will be known as the SVG duty. The chair of the SVG will organise this rota. The majority of the time the chair will be on duty, if not available one the deputies will take duty, if none are available another RAT member may be able to take on a duty.

Note that SVG does not guarantee cover on all working days, but will aim to do so. SVG does not guarantee out of hours support, or cover over public holidays – but most members do check their e-mails and will deal with any serious or urgent problems on a best effort basis.

6.3. When a potential issue is reported

Anyone may report an issue – by e-mailing report-vulnerability at egi.eu

The SVG duty should do the following:

- Acknowledge the reporter.
- Contact the provider of the software (unless the issue is quickly deemed invalid).
- Ensure that the issue is in the tracker.
- Alert the Risk Assessment Team (RAT) that a new issue has been reported by e-mail including "RAT alert" in the title.

This should happen as soon as possible, typically within an hour or two, or at least within 1 working day.

6.4. If information has been made public

Although we ask people to take care when discussing vulnerabilities it is important to consider the case where information may have accidentally or intentionally been made public. If this happens, then we should consider a special process for dealing with this. If possible, such as if it is on a web page managed by people contributing to or related to EGI, the information should be removed. When assessing the risk, if information is public it may be that the issue is placed in a higher risk category than it would be if the RAT were confident of its privacy. In most cases, CSIRT will be informed that the vulnerability has been disclosed and in what way it has been disclosed.

6.5. Investigation of an issue

The SVG RAT along with the reporter and the provider of the software investigate whether or not there is a vulnerability.

If there is not a problem at all, the issue is closed. If the issue needs attention but is not a software vulnerability, then appropriate action is taken as described e.g. in section 4.5.

6.6. Risk Assessment

If the issue is valid a Risk Assessment is carried out by the RAT which discusses the impact of each issue. The SVG duty will call for a Risk Assessment. For each valid issue, the Risk Assessment Team places the issue in one of 4 Risk Categories

- Critical
- High
- Moderate
- Low

The category is established by vote, i.e. the RAT members vote in which risk category an issue should be placed. Usually a clear majority of the votes are for a particular risk category, which is then taken as the resulting risk category. When the votes remain divided after ample discussion, in some cases the more conservative (i.e. higher) level is taken, or the matter may end up deemed out of scope for the SVG as explained in section 3.3. In some cases the CSIRT may be asked to consider an operational advisory.

6.7. Target Date Set

When the Risk has been established, the SVG on duty sets the Target Date (TD) for fixing, according to the risk category, as below.

- Critical – 3 days
- High – 6 weeks
- Moderate – 4 months
- Low – 1 year

This is from the day that the risk category is set. The reason for this is to allow the prioritization according to severity and timely fixing of vulnerabilities in the software. The SVG duty will then:

- Set the risk and TD in the tracker
- Alert the software supplier, EGI middleware unit, and reporter of the risk category and the TD.

The SVG aims to reach this point, i.e. where the risk category is set, within at most 4 working days, of an issue being reported. For critical risk issues, the aim is to reach this point within 1 working day if possible (see section 4.3).

6.8. Provide help and advice where needed on how to resolve an issue

It is not an SVG task to fix vulnerabilities. Some members of the SVG RAT are drawn from development teams, so they may happen to be involved. However the SVG RAT will provide help and advice on how to fix or mitigate problems whenever possible.

6.9. Draft Advisory

The SVG duty produces a draft of the advisory, with input from RAT members, the software provider and reporter as appropriate. The contents should be agreed with the software provider and the Risk Assessment Team.

The SVG duty puts a placeholder file on the web page – containing no information except to state that this has not been released yet.

6.10. When the software is released/or on the target date

The SVG duty makes any modification necessary to the advisory, e.g. to refer to the release notes, states the date of release and uploads it to the web page. The EGI CSIRT Team and NGIs, (TBD who else?) along with the reporter of the issue will then be informed of the availability of the new advisory.

7. Software providers view and responsibilities

7.1. Software providers agreed to an SLA

By having their software in the UMD, software providers should have agreed to a Service Level Agreement (SLA) with includes agreeing:

- That any suspected vulnerabilities found in their software are handled using the EGI SVG issue handling process.
- To provide contact details for their development teams.
- To respond when asked by the SVG as soon as possible – or at least within 2 working days.
- To co-operate to ensure that if they find a vulnerability in their own software, they fix it in a timely manner and ensure that the new version is available in the UMD for an appropriate amount of time prior to releasing information on this.

A revised version of this process document will be made available when the SLA is in place referring to the SLA.

7.2. Software providers supply up to date contact details

Software providers should ensure that they provide up to date contact details so they can be contacted as soon as possible in the event of a potential vulnerability being reported for their code.

It is recommended that software providers supply e-mail addresses both of development teams and of an overall responsible person. This should ensure that developers can be involved in the investigation whenever possible, and the overall responsible person for the software suite is alerted to any potential problems when they occur.

7.3. Software providers co-operate with the investigation

The providers of the software will be alerted with an e-mail with a title including
“SVG Alert – Possible Vulnerability in software”.

Software providers should:

- Respond as soon as they see the e-mail.
- Respond anyway within 2 working days, preferably 1 working day for issues deemed Critical.
- Help with the investigation as to whether the issue is real or not, and in what circumstances it may be exploitable

If the investigation concludes that there is a software vulnerability then:

7.4. Await Risk Assessment

The development team may usually wait for the risk category and TD to be set by the RAT.

7.5. Ensure a fixed version is available by the Target Date

It is the responsibility of the software providers to try and ensure a version free from the vulnerability is available in the UMD by the target date. The developers may consult the SVG who will help where they can with advice on how to fix the problem, and will need to co-ordinate with the UMD to ensure that the software is released on time. The software provider will also need to make it clear to the UMD when a new version fixes a vulnerability.

7.6. Review advisory

The advisory should be agreed between the development team and the RAT.

7.7. When software providers find a vulnerability

If a software provider team finds a vulnerability in their own software, they must ensure appropriate action is taken to resolve the vulnerability in a timely manner. They must ensure that a fix can be made available in the UMD prior to disclosing information on this vulnerability. There are two ways this may be achieved:

7.7.1. Inform SVG as soon as they find the vulnerability

This is what SVG would strongly prefer. This is important because there is always the possibility that if the developers can find the problem others could, especially as the software provided by the UMD is mostly open source. If this is done, the vulnerability is handled in the same way as other vulnerabilities. This also has the advantage to the development team of being able to ask the SVG for any help and advice needed in resolving it.

7.7.2. Fix the vulnerability prior to informing SVG

Some software providers will inevitably fix the vulnerability prior to informing SVG. If this is done, the software provider should report it to the report-vulnerability at egi.eu list after they have fixed it, explaining the problem and how it has been resolved. The SVG RAT will then carry out a risk assessment and set the target date in the usual way. The RAT and the development team should agree on an advisory, which will be released when the fixed version of the software is available in the UMD. If software providers take this approach they need to be aware that if there were to be an incident whereby such a vulnerability is exploited and they had delayed fixing it, it would be bad for both the EGI project and their own reputation.

7.8. Software providers are invited to join the SVG

Members of the RAT are drawn from sites, NGIs, and software providers. Software providers are invited to provide a RAT member. The workload induced on a RAT member should only be a small percentage of that person’s time. It would be best if the RAT includes members from all the major software suppliers to maximize the knowledge base of the RAT and efficiently investigate and assess problems. One incentive to provide membership is the opportunity to influence the process as well as helping to provide a secure infrastructure.

8. EGI Middleware Unit view and Responsibilities

As the focus of the EGI SVG will be on ensuring that the software released in the UMD is as secure as possible, and the issue handling is focussed on this, the EGI Middleware Unit who will inevitably need to interact with this process.

8.1. The EGI Middleware unit will be alerted when a Risk Assessment is complete

The SVG will alert the EGI middleware unit when a risk assessment is complete, stating the target date for fixing of the problem, and the software involved.

8.2. The EGI Middleware Unit and Software provider work to provide a new version in time on TD

The EGI Middleware Unit and the software provider will need to co-ordinate their work to ensure that a new version of the software, with the vulnerability fixed, is available in the UMD on or before the target date. In some cases, such as issues categorized as critical or high risk, an emergency release may need to be made available.

8.3. The EGI Middleware unit informs SVG when about to release a version which fixes a vulnerability

The EGI Middleware unit should inform SVG when they are about to release a version which fixes a vulnerability. This allows SVG to complete the advisory as appropriate and refer to the release version.

8.4. The EGI Middleware unit ensures release notes refer to the advisory

The Release notes should refer to the advisory (just as the advisory refers to the release notes).

9. CSIRT Team view and responsibilities

As well as the EGI CSIRT Team, which handles security operations related to the EGI infrastructure, various NGIs and Sites have their own CSIRTS. These may, of course, report vulnerabilities.

9.1. CSIRT Team may report a vulnerability

CSIRT members may find a security problem that turns out to be due to a vulnerability, in which case they may report it as in section 5.

When the IRTF is handling incidents, if an incident turns out to be due to a software vulnerability in the UMD distribution, they should report it to the SVG. A vulnerability that has caused an incident is likely to be classed as critical or at least high risk.

9.2. CSIRT Team will be informed if a vulnerability is assessed as critical

If the SVG identifies a vulnerability that is Critical, then CSIRT is informed. If it is not possible to produce a fixed version of the software on a short timescale, SVG will work with CSIRT to decide how best to mitigate the problem.

9.3. CSIRT Team will be informed when advisories are issued

SVG will inform CSIRT whenever it issues an advisory.

9.4. CSIRT Team will be informed of issues which cannot be fixed

This may be because there isn't a practical way of fixing it, or the problem is part of the design of the system. In this case CSIRT will be informed, with recommendation of any mitigating action that should be taken or problems they should be alert to.

9.5. CSIRT Team may consult the SVG RAT

CSIRT Team may see the RAT as a resource and consult the RAT where appropriate. This may include if the IRTF is investigating an incident and they wish the RAT to investigate some of the software. This may also include a request for an opinion on a vulnerability which is not part of the EGI UMD middleware. In general, the CSIRT Team, the subset the IRTF and the SVG will work together to ensure that any possible problem is investigated, and the deployed infrastructure is sufficiently secure.

10. NGI/Sites view and responsibilities

10.1. Sites should install up to date software

Sites should ensure that software is up to date, including installing up to date versions of the middleware distributed by the EGI/UMD and take note of appropriate advisories. Sites should be aware that CSIRT has the power to suspend sites from the infrastructure if they fail to apply critical security updates, however they should be given due warning and instruction on appropriate action to take to avoid suspension.

Advisories are issued publicly on the web at

http://www.gridpp.ac.uk/gsvg/advisories/

TBD- this may move to an EGI Wiki –

This may be publicly readable Or

This may be only readable by people who are members of the EGI CSIRT Team, NGIs and other appropriate groups.

10.2. Sites should report any vulnerabilities they find

If a site finds a vulnerability, it should be reported as described in section 5.

10.3. NGIs and sites are invited to join the SVG

The RAT is drawn from both Sites and NGIs, and software providers. NGIs and sites are invited to provide a RAT member, the workload induced on a RAT member should only take a small portion of that persons time. An incentive to provide membership is the opportunity to influence the process as well as helping to provide a secure infrastructure.