EGI Strategy and Vulnerability Issue Handling Procedure

Author:	Linda Cornwall/STFC
Version:	1
Document Link:	https://documents.egi.eu/document/2538

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author/Partner*
V 0.1	02/07/2015	First Draft for EGI engage	Linda Cornwall STFC
V 0.2	15/07/2015	Second draft, after Mischa Salle's comments. Lots of points for discussion.	Linda Cornwall STFC
V 0.3	16/07/2015	Addressed Maarten Litmaath's comments plus some discussion. (Still a lot to discuss before wider distribution)	Linda Cornwall STFC
V 0.4	22/07/2015	Addressed Mischa and Maarten's last comments. Cloud and VM stuff improved – but probably not finalized. Simplified VO section.	Linda Cornwall STFC
V 0.5	27/07/2015	Addressed Enol's comments.	Linda Cornwall STFC
V 0.6	31/07/2015	Moved 'Main handler' description to section 1, Improved 1.4. Added subsection 11.2.	Linda Cornwall STFC.
V 0.7	07/09/2015	Updates after discussion at CSIRT F2F, including releasing advisories on TD.	Linda Cornwall
V 0.8	07/09/2015	Policy violation – don't risk assess	Linda Cornwall
V 1	17/12/2015	OMB approval	

TERMINOLOGY

The EGI glossary of terms is available at: https://wiki.egi.eu/wiki/Glossary

Commonly used and additional terminology

Abbreviation	*Term*	*Explanation/info*
AppDB	EGI Application Database	
CSIRT	(The EGI) Computer Security Incident Response Team	Responsible for operational security in EGI
IRTF	Incident Response Task Force	Subset of CSIRT who take duties as security officer for EGI
RAT	The (SVG) Risk Assessment Team	This group handles vulnerabilities and has access to all information in vulnerability handling tracker.
SPG	(The EGI) Security Policy Group	
SVG	(The EGI) Software Vulnerability Group	
TLP	Traffic Light Protocol	https://wiki.egi.eu/wiki/EGI_CSIRT:TLP
TP	Technology Provider	Any member of team or organisation providing software.
UMD	Unified Middleware Distribution	Distribution of software enabling or used in the EGI infrastructure http://repository.egi.eu/

Contents

1 Introduction

1.1 Purpose

1.1.1 Purpose of the EGI Software Vulnerability Group

The Purpose of SVG is "To minimize the risk to the EGI infrastructure arising from software vulnerabilities".

The largest part of this is the handling of vulnerabilities found or reported which are relevant to the EGI infrastructure. These may be in any software which is used on the EGI infrastructure e.g. Operating Systems, Software enabling the sharing of distributed resources, VO specific software, Grid Middleware, Cloud enabling Software, AAI software.

1.1.2 Purpose of this document

The main purpose of this document is to describe the EGI Software vulnerability Group issue handling procedure, including how to report a vulnerability, which steps are carried out, and the responsibilities of the various parties involved. This includes software vulnerabilities both 'discovered' in software, as well as vulnerabilities announced by software providers.

In addition, it briefly describes other strategies for minimizing the risk due to vulnerabilities.

It would be a very long document if it was attempted to describe all possible situations, and situations occur which have not been anticipated. So the procedure should be seen as the usual way of doing things, as the way things are done unless there is a good reason to do otherwise, rather than something that must be rigidly adhered to.

1.1.3 Reason for revision

Previously during EGI-InSPIRE the main focus of the EGI issue handling was on the Grid Middleware distributed in the EGI UMD, and additionally to assist EGI CSIRT in the risk assessment of other software vulnerabilities, mainly in the Linux operating system Technology is changing, in particular related to the emergence of the EGI Federated cloud. A much wider variety of software is in use such as Cloud enabling software, software within VMs, VMs themselves, VO specific software. Some of this software is commercial produced by large or small companies or organisations; some is produced by our collaborators. Some software is released in the EGI UMD by resource providers with which EGI has a service level agreement, some such as operational tools for EGI infrastructure is released by the EGI team, as well as VOs which take their software from a much wider variety of sources. This means we need to revise the way we minimize risk arising from software vulnerabilities to the EGI infrastructure.

Recent vulnerabilities, which do not fit in with the previous procedure, have been considered when writing this revised procedure.

Note that this is the first EGI-Engage version, and revision is planned after more experience with handling vulnerabilities in the changing situation.

1.2 'Vulnerability Assessment'

1.2.1 What is 'Vulnerability Assessment'

Vulnerability Assessment is the pro-active examination of software to find vulnerabilities that may exist.

1.2.2 Vulnerability Assessment in the past

Previously a number of pieces of software, mostly provided by projects or organisations with which we had a Service Level Agreement, were assessed in detail to find any vulnerabilities which may be present. Selected software was typically software where a security problems was likely to be exposed to users, such as those which enabled the Grid infrastructure to work.

1.2.3 Vulnerability Assessment in the future

There is no budget within EGI to carry out vulnerability assessment of software. If other organisations carry out such assessments to software on which EGI depends then this is valuable to us. Generally, other strategies need to be found for ensuring that software selected for use on the EGI Infrastructure is of acceptable quality and under sufficient maintenance to minimize the risk to the EGI infrastructure.

1.3 Strategy

1.3.1 Cannot control what software is on the infrastructure

EGI SVG cannot tell people what software they may or may not deploy on their resources. This includes both resource providers, VOs and others. Nor does EGI or SVG have the resources to carry out security checks on all software which people may wish to deploy. Hence we have to accept that software will be on the EGI infrastructure which has not been selected or assessed by EGI or any of the security teams, but we still need to minimize the risk from vulnerabilities concerning that software.

1.3.2 Developers and those selecting software for deployment consider security

We ask all those who develop software, or select software for use on the infrastructure, or deploy software, or software may impact the infrastructure, to think very carefully about this software and the security implications. This includes how well it is written, as well whether it is under appropriate maintenance, and how that maintenance will continue into the future. To help we

provide a simple checklist of points which should be considered when writing software or choosing to deploy software. See section 2.

1.3.3 Carry out vulnerability issue handling according to procedure

If vulnerabilities in software which is deployed in the EGI infrastructure, or impacts the infrastructure, vulnerability issue handling is carried out according to the agreed procedure in this document.

1.3.4 All parties must comply with the relevant Security Policy

The EGI Security Policy Group (SPG) aims to provide policies that define the expected behaviour of sites and users to ensure a secure distributed computing infrastructure. [R 1] All parties are expected to take responsibility for their own actions, and consider the security implications of any software installed and configured. Some of the security policies say 'Grid', they do apply whatever technology is being used in the shared distributed computing infrastructure.

1.4 SVG, Technology Providers (TPs), and Scope of SVG.

For some software, such as software distributed by EGI, in particular in the EGI UMD, the EGI SVG is the main handler (see section 1.5) of vulnerabilities in this software. Vulnerabilities discovered including those which have not yet been fixed are reported to SVG, and handled fully as defined in this document.

The SVG may also carry out software vulnerability handling for collaborating organisations that provide software used to enable the EGI infrastructure.

Any organisation providing software with which EGI has an SLA, it is compulsory to co-operate with the EGI if potential vulnerabilities are found.

The other main activity is to handle vulnerabilities in software which is widely used in the EGI infrastructure, whether produced commercially or not. Mostly vulnerabilities in such software are announced after resolution (although of course zero day vulnerabilities occur at times) and SVG's role is to consider the risk in the EGI infrastructure, rather than arrange for resolution. Rarely vulnerabilities are found in such software are initially reported to SVG, in this case SVG passes the information to the software provider.

For other software, such a VO specific software, SVG's role is remains to minimize the risk due to vulnerabilities. This is by providing the checklist in section 2 and handling any vulnerabilities reported in this software. Those selecting or deploying the software take the prime responsibility in this case.

1.5 SVG as the 'main handler' of the vulnerabilities for a given technology

When we say SVG is the 'main handler' we mean that when people 'discover' a vulnerability the means of getting it fixed is primarily by reporting it to SVG. This is unlike, for example, other software providers who provide software which may be used in the EGI infrastructure as well as many other places, where EGI is likely to be one of a large number of infrastructures which use it. If SVG is the 'main handler' SVG investigates, contacts the technology providers and developers, carries out a risk assessment and based on the risk sets a Target Date by which time the vulnerability should be fixed. This is the case for software developed by EGI, and released in the EGI UMD.

SVG may be the main handler of other software from collaborating projects, who are developing software to enable the EGI infrastructure, but this is not compulsory.

For software from other organisations, e.g. where EGI is only one of a number of infrastructures using the technology, the technology provider will probably have its own system for handling vulnerabilities found and EGI normally only considers announcements of vulnerabilities. EGI is probably 'invisible' to such organisations. Most such vulnerabilities will be announced in this way.

Some are in-between, are aware of us but have their own handling procedure. Generally we have to act according to the circumstances.

1.6 Relationship between SVG and CSIRT

In the past SVG handled Grid Middleware issues, whereas CSIRT handled issues concerning operating systems. Now all CSIRT members who take a duty as 'Security officer on duty' are in the SVG RAT, and all issues regardless of what type of software they concern are handled by the SVG RAT.

The EGI Security officer, and any other member who takes on the role as 'Security officer on duty' may act quickly in any way they see appropriate concerning vulnerabilities without consulting the rest of the SVG. This may include advising sites to patch or stop using a particular piece of software if they wish.

All CSIRT members including those who do not take on a duty as 'security officer on duty' are invited to join the SVG RAT if they wish.

1.7 Caveats

The purpose of SVG is "To minimize the risk to the EGI infrastructure arising from software vulnerabilities", and this is what we aim to do. SVG cannot guarantee that something important won't be missed. There is no 'out of hours' cover, although some members may look at urgent issues out of hours. Manpower is limited: for example we cannot guarantee that all issues are

handled as quickly as we might like, e.g. if several issues are reported at once the ones which appear more serious will have to be given priority.

EGI provides some funding for the co-ordination of SVG. The success of SVG also depends on various collaborating institutes and organisations allowing and encouraging their staff to participate as RAT members, who carry out the investigation of issues and risk assessments.

Note that it is no-one's responsibility to trawl CVE's, looking for ones that may be relevant.

Note that this procedure will be reviewed again at some point in 2016 after experience of using it.

1.8 Procedure on wiki

A summary of the SVG issue handling procedure will be placed on the EGI public wiki.

This document does not describe the specific tools used for handling vulnerabilities. Note also that details such as templates for handling vulnerabilities are not in this document. Nor are contact details for software providers, these are maintained separately.

2 Software Security Checklist

People often develop or select software because it does something useful, which they wish to do. The motivation is to get things working, do something useful, and security is often not considered.

Anyone who is developing software, or selecting or deploying software on the EGI infrastructure, or which may have an impact on the EGI infrastructure needs to consider security. We will maintain this simple checklist to help, and it will additionally be placed on the wiki.

This should apply to anyone selecting or writing software for use on the infrastructure, whether resource providers, VOs, or those selecting or writing software for the enabling of the sharing of computing resources in EGI.

2.1 Who is the Technology Provider?

If the Technology Provider (TP) is a large organisation or company, with a good record for providing good, reliable, secure software then this is good.

The large linux distributions usually redistribute software which others have provided, but the distributions themselves typically have good vulnerability handling procedures and strategies which can be relied on

If the technology provider is a group of people we know well, with a good track record of producing reliable secure software and the programmers have good skills and are co-operating with the project to provide software suitable for use then this is good indicator that the software is should be considered for use.

In the case of unknown, small companies, 'hobby' programmers, and other software which you may come across and think 'this is useful' think carefully and be extra vigilant and sections 2.2, 2.3, 2.4, 2.6, 2.7, 2.8, 2.9 need to be considered very carefully.

2.2 Has anyone with security expertise done an assessment of it?

If an assessment has been made by people with security expertise consider their findings.

2.3 Does the code look good?

If the software has not been produced by a large reliable company or organisation then take a look at it. See if it looks good, clear, and maintainable?

2.4 Is user input sanitized?

Some of the commonest types of software vulnerability come from the failure to sanitize user input. These include buffer overflow vulnerabilities and sql injection vulnerabilities. It is not

sufficient to trust a client supplied by a software provider. New malicious clients may be developed. This is particularly important if the programming language used and the software itself contains constructs which may be exploited if user input is not sanitized.

2.5 Can you ensure that using this software complies with EGI Data protection policy?

The EGI data protection policy is currently being developed. It is essential to comply with data protection legislation. As a bare minimum it must not be possible to link an action to an individual user, and make this information widely available.

2.6 Is the software under security support?

If the infrastructure depends on some software it is important that it is under security support. Consider the type of security support – if it's a large reliable company then it's likely to be fine.

If the programmers are from a collaborating project and are funded to continue to develop and maintain this software then it is also likely to be fine.

If the software is provided by a small company, which you know little about then look carefully at how well it's likely to be supported.

If the software support is no longer funded the institute providing it is willing to support it and their programmers maintain it during work time then it is likely it will be O.K.

If it's not supported, or relies on someone maintaining it as a hobby then think again about whether security support or for that matter other support is adequate.

2.7 How long will the software be under security support?

It may be that a large company or organization commits to supporting the software for a number of years into the future. If so, then this is good. Otherwise, think about how long support is likely to be available.

2.8 When was the last stable release?

If the last stable release was several years ago, it is probably an indication that support may actually be limited and cannot be relied upon.

2.9 How are software vulnerabilities handled?

It is essential that a new vulnerability can be reported to the technology provider, without generating a publicly readable ticket or other publicly available information. That this is done and how should be checked.

For a large company or organization the creation of a ticket, or a security e-mail address may be provided. For a smaller organisation, or collaborating project, directly e-mailing the developers may be the means of reporting vulnerabilities.

2.10 What are the configuration issues related to security?

Check the configuration issues related to security, and ensure that the software can be configured securely in the circumstances in which you wish to use it and that it complies with the EGI data protection policy.

3 Vulnerability issue handling procedure

The Issue handling is carried out by the SVG-RAT. See section 10.3

3.1 Basic procedure

3.1.1 Reporting a vulnerability

Anyone may report a vulnerability by e-mail to:

report-vulnerability@egi.eu

This may be used for any vulnerability which is discovered in any software used or relevant to the EGI infrastructure, or announced by the technology providers if it is thought appropriate to alert SVG to it. For more details see section 4.1

3.1.2 Investigating a vulnerability

The RAT, along with the reporter (if applicable), and the technology provider (if appropriate) and any other appropriate party investigate the issue. If it is found to be valid the relevance and effect in EGI is determined.

3.1.3 Risk assessment

If the issue is valid and relevant to EGI, a risk assessment is carried out by the RAT. The issue is put into one of 4 risk categories 'Critical', 'High', 'Moderate' or 'Low'.

3.1.4 Set Target date for resolution according to Risk

If the issue has not been fixed, a Target Date (TD) for resolution is set according to the risk category as below.

- Critical – Special procedure – see sections 3.2 and 7
- High – 6 weeks
- Moderate – 4 months
- Low – 1 year

This target date is the date by which software free from the vulnerability should be available for installation in all appropriate repositories. This allows the prioritization for the timely fix of software vulnerabilities.

3.1.5 Fixing the issue

If the issue has not already been fixed, it is then up to the software provider and the appropriate release team to ensure software free from the vulnerability is available for installation in the appropriate repositories by the target date.

3.1.6 Advisory issued

An advisory is issued:

- If EGI SVG is the main handler (see section 1.5) of vulnerabilities concerning this software, regardless of the risk
    - When it is fixed
    - On the Target date if it is not fixed by then
- If the issue is assessed as 'High' or 'Critical' risk
- If the EGI SVG considers it useful to alert sites

The advisory is sent to site-security-contacts@mailman.egi.eu ngi-security-contacts@mailman.egi.eu noc-managers@mailman.egi.eu svg-rat@mailman.egi.eu csirt@mailman.egi.eu plus the reporter, and anyone else or any list seen as appropriate to cc. See section 10.5 for more info on where to send advisories.

- For 'High' and 'Critical' vulnerabilities which are NOT already publicly disclosed advisory is sent as TLP 'Amber' See [R 2]
    - It is made public 2 weeks after it is fixed to allow software to be updated prior to making information public and placing on the public wiki.
- For all other issues sent as TLP 'White', and placed straight on public wiki

3.2 Special procedure for critical vulnerabilities

In the past it has been stated the 'Target Date' for fixing critical vulnerabilities is 3 working days, but in reality this may not be realistic. What action is taken is dependent on the circumstances: the patch may have been 'announced' by the software provider, or a reasonable work-around may be found, or we may decide to wait a few days for a patch. More details are in section 7.

3.3 Issues not fixed by Target Date

If an issue reported to SVG is not fixed by the target date, the action taken will depend on the circumstances and the risk associated with the vulnerability.

This is a change from the previous procedure, see section 10.4

3.3.1 Contact software provider

The software provider will be contacted, and asked for an update. The software provider will be reminded that the issue is near or past the Target Date, and of the importance of fixing vulnerabilities.

3.3.2 Advisory released as 'Amber' for 'High' risk vulnerabilities.

The advisory will normally be released as 'Amber' to inform sites of the problem. As the OMB is included in the distribution list management is effectively informed of this. The info will remain 'Amber' until a final solution is found. The advisory may include recommendation for mitigating action if appropriate.

3.3.3 Release of advisory for 'Moderate' and 'Low' risk vulnerabilities.

Advisories will normally be released for 'Moderate' and 'Low' risk vulnerabilities on or shortly after the TD. Exceptions may be made if the software provider states that the fix is in work and able to provide a date when they plan to release the fixed software.

4 Details for reporter of vulnerability

4.1 Not publicising vulnerabilities

It is important that information on vulnerabilities is kept private while they are investigated and while the software providers are fixing them. Hence when new vulnerabilities are discovered they 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 publicly readable web page.

For vulnerabilities discovered by the reporter of the vulnerability (as opposed to those announced by the technology provider) it is important that the technology provider is informed of them, without releasing information publicly. If an EGI user or other person who participates with EGI finds a vulnerability in software which is used in or relevant to the EGI infrastructure it MUST be reported to the EGI Software Vulnerability Group as in 4.2. Additionally, it may be reported via the means defined by the technology provider (see section 2.9) if such means have been defined. If this additional reporting to the technology provider is not carried out SVG will report to the software provider. It is very helpful if the reporter tells SVG whether or not they have additionally contacted the technology provider, who, and by what means.

4.2 Reporting a vulnerability

Any suspected software vulnerability which is relevant to the EGI infrastructure should be reported to:

report-vulnerability@egi.eu

Please report by this means. This creates a ticket in the SVG tracker which is readable by all SVG RAT members. (See section 10.3)

This is true if you discover a new vulnerability, or if you think an announced vulnerability is relevant to EGI.

If a newly discovered vulnerability is reported to the SVG tracker, the information will be passed onto the technology provider if it hasn't been already.

4.3 Reporter may help with investigation

It is very helpful if the reporter of a vulnerability helps with the investigation and handling by SVG. Due to the expansion of software in the infrastructure, SVG members will not know about all the software in use, so all those with knowledge who help with the activity can contribute to making it a success.

4.4 Reporter receives feedback

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.

4.5 Reporter is acknowledged

The reporter will be acknowledged if an advisory is issued, unless the reporter explicitly asks not to be.

5 Details for SVG RAT members

Templates for various mails and advisories will be maintained on the wiki. Other details will also be on the wiki where it is suitable for it to be public. Details such as e-mail addresses for certain contacts will be kept elsewhere.

5.1 When a potential vulnerability issue has been reported

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

The SVG duty should do the following

- Acknowledge the reporter
- Contact the developers or technology provider with appropriate information, unless
  - The report is clearly invalid or
  - The technology provider obviously knows about it because e.g. their representative is informing you, or the vulnerability has been publicly announced
- In the case of VO specific vulnerabilities, also inform the VO security officer
- Ensure that the issue is in the Software Vulnerability Issue tracker, (if it has not been reported via the report-vulnerability e-mail).
- 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

5.2 Investigation of the issue

If the issue is a new, non-announced vulnerability, investigation should be carried out to find if the issue is valid and the effect. It is important that the technology provider is involved in this.

All vulnerabilities should be investigated to understand the likely effect in EGI infrastructure.

Note that not all cases are straight-forward, and not all can fit neatly into a procedure or be anticipated. The information in section 11 ‘dealing with certain situations’ may be helpful.

5.3 Risk Assessment

This may be done in parallel with 5.2

If the issue is valid and relevant to EGI a Risk Assessment is carried out by the RAT which discusses the impact of each issue in the EGI infrastructure. For each valid issue, the RAT 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, or a consensus is reached, which is then taken as the resulting risk category. When the votes remain divided after ample discussion, the higher level should be taken.

The Risk Assessment should be discussed on the RAT list, not in the tracker entry, and a summary placed in the tracker entry.

5.4 Set Target Date for resolution

If the issue has not been fixed, then a target date is set from the time when the Risk has been established. The Target Date (TD) for fixing is according to the risk category, as below.

- Critical – special process – see section 7
- High – 6 weeks
- Moderate – 4 months
- Low – 1 year

This is to allow the prioritization according to severity and timely fixing of vulnerabilities in the software.

5.5 Inform Technology Providers of the outcome

If a TD is set, inform the technology provider of the outcome of the risk assessment and target date.

SVG aims to reach this point, i.e. where the risk category is set and the TP informed, 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

SVG members should provide help and advice if necessary and have the appropriate skills and knowledge.

5.6 Draft advisory

Draft an advisory if one is needed.

An advisory is issued if:

- SVG is the main vulnerability handler (see section 1.5) for this technology, regardless of risk
- If the issue is ‘High’ or ‘Critical’

- If there is some other reason e.g. publicity, the risk may rise if public exploits become available, or any other reason where SVG considers it appropriate to issue an advisory.

If EGI is the main handler of vulnerabilities for this technology, or is in contact with the TP, then ask them to comment. Take advice from anyone appropriate.

For 'announced' vulnerabilities these may be very simple, stating the risk in the EGI environment and referring to the TP advisory.

5.7 Issue advisory

The advisory should normally be issued when the vulnerability has been fixed. This may be very soon in the case of an 'announced' vulnerability, or may be when a new version of the software is released hopefully before the target date.

The advisory is sent to site-security-contacts@mailman.egi.eu ngi-security-contacts@mailman.egi.eu noc-managers@mailman.egi.eu svg-rat@mailman.egi.eu csirt@mailman.egi.eu plus the reporter, and anyone else seen as appropriate to cc.
For issues announced concerning Linux distributions, this should additionally include VM Operators and VM Endorsers. See section 10.5

- For 'High' and 'Critical' vulnerabilities which are NOT already publicly disclosed advisory is sent as TLP 'Amber' See [R 2]
    - Then made public 2 weeks after it has been resolved to allow software to be updated prior to making information public and placing on the public wiki.
- For all other issues sent as TLP 'White', and placed straight on public wiki

Additionally in principle advisories should go to VM endorsers and VM Operators. At present the exact lists and where they go to is still in discussion.
Advisories are sent regardless of risk for issues where SVG is the 'Main Handler' (see section 1.5)
For announced issues advisories are sent if the risk is 'High' or 'Critical' or there is other good reason why it makes sense, such as SVG had already sent a 'heads up', or the vulnerability has attracted a lot of publicity.

Timing of sending advisories should be considered. Only 'Critical' should be sent outside working hours. Others should be sent at a time where the majority of the people in Europe are at work, preferably mid-morning or mid-afternoon, and avoid Friday afternoons if possible.

5.8 Other SVG responsibilities

5.8.1 Ensuring infrastructure for issue handling is available

The procedure depends on various mailing lists, contact details, templates, wiki and the tracker. Most of these are via the EGI facilities. It is the responsibility of SVG to ensure these are maintained.

5.8.2 Engaging with Technology Providers and people installing software

SVG should attempt to engage where possible with Technology Providers and groups of people installing software to ensure they are aware of the need to provide and install secure software. This may be by presentations at conferences or meetings, alerting people to wiki pages and other information.

This includes ensuring that contact details for various TPs on which the enabling of shared resources in the EGI infrastructure depends are available so people can be contacted quickly if there is a problem.

5.8.3 Providing rota if possible for issue handling

Where possible, during working days, the SVG chair should ensure someone is available to handle issues reported. This cannot be guaranteed, and the fact that the IRTF members are also in the SVG-RAT means the security officer on duty is the default for dealing with urgent issues if no other SVG-RAT member is available.

5.8.4 Providing reports to EGI management as required

As title.

6 Details for Technology Providers

Technology providers (TPs) are anyone providing a technology which has an impact on the EGI infrastructure.

For the majority of TPs, EGI SVG is effectively invisible. Large technology providers announce vulnerabilities when they are patched. The EGI SVG simply takes information provided by them. Very rarely a vulnerability may be reported to us by the 'discoverer' in which case we will pass information on.

Some TPs are specifically writing software for use on the EGI infrastructure and other similar infrastructures. They are aware of SVG, many of which EGI may have an SLA and for many EGI SVG is the 'Main handler' (see section 1.5) of software vulnerabilities. This section is largely aimed at this group. We define EGI itself as a technology provider, and the persons who maintain software in the EGI UMD as technology providers.

VM Endorsers may also be seen as technology providers, see section 9.1.

6.1 Ensure up to date information on contact details is available to SVG

It is important that software providers can be contacted and vulnerabilities reported quickly and easily without generating public information. This may be, for example, via a security e-mail list, e-mail directly to specific developers, or a ticketing system which allows private tickets to be created which are only viewed by appropriate developers. This must be easy for SVG to find. This may be simply informing SVG who to e-mail in case of security problems, (in particular for TPs with which we have an SLA) or informing SVG of a security mailing list.

6.2 Technology Provider should take care of sensitive information

The Technology provider should take care not to disclose information that may be useful for attackers. For example vulnerability information should not be disclosed in a public bug tracker. The version control system should not say 'fix for critical remote root exploit', before information has been made public as part of the vulnerability handling procedure.

6.3 Be ready to investigate a potential vulnerability when reported

If a potential vulnerability is reported the TP needs to investigate as soon as possible. Now that a much wider variety of software is being deployed on the EGI infrastructure it is not reasonable to expect SVG members to be expert in everything, so the TP will be increasingly relied upon to establish what if any is the problem with software. The TP is trusted to do this honestly.

6.4 If the vulnerability is confirmed, fix it by the Target Date

If the vulnerability is confirmed SVG will carry out a risk assessment and set a Target Date (TD) for resolution according to the risk (see section 3.1.4). Please ensure the vulnerability is fixed by this time, and that the fix is fully released by this time ready for widespread deployment.

6.5 Review advisory

SVG will draft an advisory. TP should review this and comment on accuracy and anything else they wish.

6.6 If the Technology Provider finds a vulnerability

It is quite common that the TP finds a vulnerability in their own software, and is able to fix it in a timely manner. It is important that TPs do take action concerning vulnerabilities they find themselves, and don't just ignore them. TPs with whom EGI has an SLA are required to inform SVG of such vulnerabilities, just as they are required to respond to SVG, this allows SVG to ensure that an advisory is available when the issue is fixed.

SVG may be informed by e-mail to report-vulnerability @ egi.eu

This creates a ticket in the tracker, and all members of the RAT will be able to see it.

There are 2 options:--

6.6.1 TP inform SVG as soon as the vulnerability is found

This is the preferred time as it allows SVG to carry out a risk assessment and draft an advisory at the earliest opportunity.

It also may be advantageous to the TP as it allows earlier information on the risk, how urgent it is to fix the issue, and in some cases SVG may be able to help TP with advice on resolving the issue.

6.6.2 TP informs SVG when the vulnerability has been fixed

This is O.K. but please inform SVG before publicly releasing the fix, to allow time for SVG to carry out a risk assessment and draft an advisory.

7 Critical vulnerabilities

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 one working day. In many cases it is more important to simply establish whether the problem is real and applicable in EGI and find a short-term solution, than decide on a long-term solution.

Note that the EGI security officer, IRTF chair, or the IRTF officer on duty may decide an issue is critical and act accordingly, without consulting others. All these are members of the SVG RAT.

In recent years there have been typically 2 to 4 critical vulnerabilities per year. The majority concern vulnerabilities in software where the TP is a large organisation, and the vulnerability is 'announced' having been resolved, or discussed publicly then resolved fairly quickly by the TP. It is then up to SVG to produce an appropriate advisory for sites, then CSIRT/IRTF to monitor for vulnerable sites. In this case only 7.2, 7.3, 7.7, 7.8 are carried out by SVG, and 7.9 by CSIRT/IRTF. Sometimes information on a vulnerability is made public without having been resolved, these are known as 'zero day' vulnerabilities, and have to dealt with as appropriate, in this case action in 7.4 may be most appropriate.

In many cases these 'steps' are carried out in parallel. These should be seen as steps that should be considered, some will be more relevant than others, some may be skipped if it is deemed urgent to get the advisory out to protect the infrastructure.

7.1 Alert all appropriate parties

Alert the Technology Provider (unless they are clearly aware of and fixing or fixed the problem), the EGI UMD Release Team (if the software is in the UMD), VO manager and security contact (if the software is related to a VO) and any other relevant party.

7.2 Consider sending a 'heads up' to sites

This is an alert to sites that a serious problem has been found and that further advice will follow. This is at the discretion of SVG RAT, the EGI security officer and the duty officer. A 'heads up' may also be sent if a technology provider announces that they are planning to release software to fix a serious security issue, again at the discretion of SVG RAT, the EGI security officer and the duty officer.

7.3 Establish the effect of someone exploiting the vulnerability

Make sure that the effect of someone exploiting the vulnerability in the EGI infrastructure is established as clearly as possible. Establish what software or combination of software/operational

configuration allows the vulnerability to be exploited in the EGI infrastructure. It may turn out that it is not possible to exploit

7.4 Find if any action can mitigate or resolve the problem

Consider whether any mitigating action can be recommended. If so draft appropriate advisory and send an advisory to recommend the mitigating action.

7.5 Find out how quickly a patch can be made available

Find out how quickly a patch can be made available. If a vulnerability is easy to solve it may be possible to get a release in hours or a small number of days. If it is complex to fix, it might take longer.

7.6 Decide whether to wait for a patch

Decide whether to wait for a patch, or whether to recommend other action.

7.7 Ensure advisory is completed ready for the software release

Draft advisory if not already done so.

7.8 Release advisory

Send advisory as in 3.1.6

If the vulnerability is not public send as TLP 'Amber' and release publicly in no less than 2 weeks.

7.9 CSIRT/IRTF carries out operational procedure for critical vulnerabilities

The issue is handled by CSIRT/IRTF according to the critical vulnerability handling procedure [R 4]

8 Virtual Organisations and Vulnerabilities

8.1 Virtual Organisations (VOs) should consider the security of any software they use

VOs should consider the checklist in section 2 and ensure the software they use or produce is suitable from a security point of view.

8.2 Vulnerabilities associated with VO or VO specific software

In this case the Technology Provider is the VO, and the VO has the same responsibilities as any other technology provider in section 6 .

If a vulnerability is associated with a VO or some VO specific software, SVG will contact the relevant VO security contact, and the VO manager from the VO-ID card in the operations portal [R 5]. SVG will also contact anyone else associated with the VO or software they are aware of and think appropriate to contact, such as developers listed in a wiki associated with that software.

8.3 VOs should ensure contact details are complete and up to date

VOs should ensure the contact information in the VO-ID card is complete and up to date.

9 Virtual Machines and Vulnerabilities

Note that this is in work/discussion.

Anyone involved in the Endorsement or Operation of VMs should see the "Security Policy for the Endorsement and Operation of Virtual Machine Images" [R 3] we use the terminology in this document

Endorser: A role, held either by an individual or a team, who is responsible for confirming that a particular VM image has been produced according to the requirements of this policy and states that the image can be trusted.

VM operator: A role, held either by an individual or a team, who is responsible for the security of the VM during its operation phase, from the time it is instantiated, until it is terminated. Typically this addresses individuals with root access on the VM.

VM consumer: A role held by an individual who consumes with no level of management privilege the services operated on or by a VM.

9.1 VM Endorser and vulnerabilities

The endorser of a VM has on-going responsibility for ensuring that the endorsed VM does NOT contain any vulnerabilities, and complies with policy as in [R 3]

The VM endorser as well as considering the policy requirements in [R 3] may additionally use the checklist in section 2 when including software in any endorsed image.

A bad Endorsed VM is seen like a vulnerability, the endorser being the TP IF either:--

- It is a case of a misconfigured VM image (e.g. containing passwords, private keys etc.)
- It is case of including vulnerable non-standard, poorly maintained software.

In this case the endorser of the particular VM will be contacted.

In the case of an endorsed VM containing vulnerable software, the endorser is seen rather like a site which has to patch, and must ensure security updates are promptly and correctly applied. For issues concerning linux distributions and other widely used software which are assessed as 'High' and 'Critical' by SVG it is planned that VM Endorsers should receive the advisories issued by SVG. It should be noted that VM Endorsers should not ONLY patch when they receive an advisory from SVG, but that these advisories are an additional activity to minimize the risk to the EGI infrastructure arising from software vulnerabilities.

Running VMs based on vulnerable endorsed VMs will be treated by IRTF in a similar way to other vulnerabilities exposed in the infrastructure, according to risk.

(Note: need a VM Endorser contact list.)

9.2 VM Operator and vulnerabilities

VM Operators are responsible as in [R 3]

VM Operator should only run endorsed VM images.

If a VM Operator adds software on contextualization or at any other point during the VM lifecycle the checklist in section 2 should be considered, and the VM operator is responsible for ensuring the security of the VM throughout its lifecycle.

It is the VM Operator responsibility to ensure that all security updates are promptly and correctly applied. For issues concerning linux distributions and other widely used software which are assessed as 'High' and 'Critical' by SVG it is planned that VM Operators should receive the advisories issued by SVG. It should be noted that VM Operator should not ONLY patch when they receive an advisory from SVG, but that these advisories are an additional activity to minimize the risk to the EGI infrastructure arising from software vulnerabilities.

9.3 VM Operators authorization and contact

It has been noted that in most cases all members of a VO which is authorized to Operate VMs in the EGI Federated cloud may become VM Operators. There is no special group or role within a VO for VM Operators. Hence in principle all members of all VOs will be able to become VM Operators.

(Note: ideally need a VM Operator contact list. How this is to be provided is uncertain. It may be that only VO security contacts are contacted. Also, more consideration needs to be made concerning 'Amber' information.)

10 Descriptions and explanations

10.1 What is a vulnerability?

There are many definitions of a software vulnerability. We usually consider a vulnerability as a problem where a principal can gain access to 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 not 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.

It does not matter whether a vulnerability is due to a coding error or a poor design.

10.2 What is NOT a vulnerability?

10.2.1 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 encrypted data alongside 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 and persons with site administrator privileges.

Note that VM Operators are not trusted in the same way as site administrators, they are only trusted within their realm e.g. concerning the VO on whose behalf they instantiate and operate VMs.

10.2.2 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.

10.2.3 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 forward information to the appropriate groups.

10.3The SVG 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 software, CSIRT members, 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 community. 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.

The EGI IRTF members who take a duty as the EGI security officer are also members of the RAT. This allows an early alert to any serious vulnerabilities reported as well as allows them to provide their opinion or comment on any issue they wish.

10.4Change in 'responsible disclosure'

In the past SVG said the advisory would be sent and made when the vulnerability is fixed or on the target date, whichever is the sooner. This is known as 'responsible disclosure' and encourages the reporting of vulnerabilities to our group. This was reasonable when the vulnerability handling procedure only really concerned Grid Middleware was very separate from the operational security group. In recent years SVG and CSIRT/IRTF have become much closer together, and SVG is now involved with all types of vulnerabilities relevant to the EGI infrastructure, and irtf members are in SVG. The main duty of SVG is to protect the EGI infrastructure, and all parties involved, so disclosing issues on the Target Date if they are not fixed may not always be in the interest of EGI. Hence now for 'High' and 'Critical' risk vulnerabilities information is sent 'Amber' if it is not already public and remains 'Amber' until at least 2 weeks after the issue is fully resolved.

10.5 Where advisories are sent to

Advisories are always sent to the following:

site-security-contacts@mailman.egi.eu
ngi-security-contacts@mailman.egi.eu
noc-managers@mailman.egi.eu
svg-rat@mailman.egi.eu
csirt@mailman.egi.eu
Plus the reporter of the vulnerability.

It is better that people ignore a vulnerability which is not relevant to them, than do not receive information on a vulnerability which is relevant to them.
Some exceptions are when information is sent as 'amber'
There is no special list for sites deploying cloud services, and for vulnerabilities concerning e.g. cloud enabling software, hypervisors etc, sites which do not deploy such software can simply ignore them.
This is similar to the way in which all sites have been receiving advisories on all grid middleware, even though some of this information is not relevant to all sites.

For advisories concerning linux or other commonly used software, in addition advisories should go to VMOperator contacts and VMEndorser contacts (at time of writing, not yet available).

11 Dealing with certain situations

While this document is intended to describe how to handle the majority of situations concerning vulnerabilities, situations may occur that have not been anticipated. It would also be very complex to try to define every possible situation.

11.1 Be aware of the purpose of the group

Whatever situation occurs which do not easily fit in with the procedure, SVG should consider what is best to do to fulfil the the purpose of the SVG which is "To minimize the risk to the EGI infrastructure arising from software vulnerabilities".

11.2 Issues concerning policy violation

If an issue is found which concerns a security policy violation, which is 'by design' rather than a simple bug, this is handled in a different way. An e-mail is sent to SCG and SPG – and the issue is primarily handled by SPG.

SVG does not risk assess these, but informs SCG and SPG. If they are resolved, or mitigating action is recommended, SVG may send an advisory.

Typically these concern the ability to read data where jobs are associated with DNs, which is against data protection legislation.

11.3 Issue which may affect multiple pieces of software

A vulnerability may be found in some software on which multiple other pieces of software depend, or which may need resolution in a number of pieces of software, and it may not be clear which and how some of the software is affected. In this case it makes sense to contact the all software providers where EGI is the ‘main handler’ (section 1.5) of vulnerabilities concerning this software. For now the ‘URT discuss’ list will be informed. In future a more comprehensive list may be available.

12 Technology and vulnerabilities

This table indicated what is done in the various cases. It is intended as a guideline, and cases that do not fit will be handled as considered appropriate.

Table 1 – Vulnerabilities and technologies

Software Source	*TP aware or vulnerability announced*	*TP not clearly aware of vulnerability*	*Risk Assess*	*Advisory Issued*	*Comments*
EGI UMD or other EGI distribution	Vulnerabilities fully handled according to this procedure		Yes	**All valid vulnerabilities**	This was what SVG was initially intended for.
Operational Tools developed by EGI and collaborators			Yes	All valid vulnerabilities	
Other software where EGI SVG is 'Main Handler' See section 1.5			Yes	All valid vulnerabilities	
Other software where EGI has SLA with TP	TP should co-operate with SVG	Inform TP	Yes	Usually all valid vulnerabilities	
Other software widely installed on EGI infrastructure	Usually the case	Inform TP	Yes	Usually only if assessed as 'Critical' or 'High'	Mostly this is 'announced' vulnerabilities. Common situation.
VO specific S/W	Also usually handle according to this procedure	Inform TP	Yes	Usually	
Software not installed on the EGI infrastructure	No action after establishing it is not relevant to EGI	Simply forward info to TP – it would be irresponsible not to forward the info.	No Risk due to being irrelevant	No	Unlikely such vulnerabilities are reported to us

13 References

No	Description/Link
R1	The EGI Security Policy Group https://wiki.egi.eu/wiki/SPG
R2	Traffic Light Protocol https://wiki.egi.eu/wiki/EGI_CSIRT:TLP
R 3	Security Policy for the Endorsement and Operation of Virtual Machine Images https://wiki.egi.eu/wiki/SPG:Drafts:Virtual_Machines_Endorsement_Policy_March_2015
R 4	EGI-CSIRT Critical Vulnerability Operational Procedure https://wiki.egi.eu/wiki/SEC03
R 5	VO operations dashboard http://operations-portal.egi.eu/vo/search