EGI Strategy and Vulnerability Issue Handling Procedure

Author:	Linda Cornwall/STFC

Version:	1.06
Document Link:	https://documents.egi.eu/secure/ShowDocument?docid=3145

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	
V 1.01	08/06/2017	Updates after various discussions and 18 months further experience.	Linda Cornwall STFC
V 1.02	06/07/2017	Accepted Maarten's proposed changes. Addressed changes from discussion with SVG especially in meeting on 28th June.	Linda Cornwall, STFC
V1.03	18/07/2017	Accepted Maarten and Ian's last lot of changes, addressed comments and discussion from meeting on 13th July	Linda Cornwall, STFC
V1.04	21/07/2017	Accepted Maarten and Mischa's proposed changes, addressed discussion and comments.	Linda Cornwall, STFC
V1.05	24/07/2017	Accepted Maarten's changes, addressed Mischa's comments.	Linda Cornwall, STFC

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	
CMD	Cloud Middleware Distribution	Distribution of software enabling the EGI Fed Cloud on top of OpenStack and OpenNebula
CSIRT	(The EGI) Computer Security	Responsible for operational security in EGI

	Incident Response Team	
CVE	Common Vulnerabilities and Exposures	A dictionary of common names (i.e., CVE Identifiers) for publicly known cyber security vulnerabilities
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	
SVG Co-ordinator	Person in SVG who ensures issue handling process is carried out	
TLP	Traffic Light Protocol	https://wiki.egi.eu/wiki/EGI_CSIRT:TLP
UMD	Unified Middleware Distribution	Distribution of software enabling or used in the EGI infrastructure http://repository.egi.eu/
VA	Virtual Appliance	(Endorsed) VM image in AppDB
VM	Virtual Machine	

Contents

1 Introduction

1.1 Purpose

1.1.1 Purpose of the EGI Software Vulnerability Group

The purpose of EGI Software Vulnerability Group (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 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, Authentication and Authorization software.

1.1.2 Purpose of this document

This document describes the EGI SVG 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.

This document is not intended to describe all possible situations but rather it aims to provide best practice guidance to be adapted to circumstances.

1.1.3 Reason for revision (2015)

Previously during EGI-InSPIRE the main focus of the EGI vulnerability 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.

Now, a much wider variety of software is in use, such as for example Cloud Frameworks. This means that as well as software produced or distributed by EGI and EGI's collaborators a lot of software produced by other companies or organisations is used on the EGI infrastructure.

These changes mean we need to revise the way we minimize risk arising from software vulnerabilities to the EGI infrastructure.

1.1.4 Reason for revision (June 2017)

The SVG issue handling procedure is revised for the following reasons:

- Minor change in the criteria for the border between 'Critical' and 'High' risk vulnerabilities.

- Additional clarification/info/steps for handling Critical vulnerabilities when a patch is not available
- Options for when it is difficult to establish risk due to lack of homogeneity
- Option of asking sites to check configuration
- Modification/improvement to some cloud related aspects, as a result of experience and changes which have occurred

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. At present there is no budget within EGI to carry out vulnerability assessment of software.

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 problem 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

If other organisations carry out such assessments on 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.

1.3 Strategy

EGI SVG cannot tell resource providers, VOs and others what software they may or may not deploy on their resources. Nor does EGI or SVG have the resources to carry out security assessments 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.

1.3.1 Security is everyone's responsibility.

Everyone who interacts with EGI is responsible for Security within their own domain. Managers, developers, users, those selecting software for use on the infrastructure, those managing data centres all have to be aware of and consider security. All parties are expected to take responsibility for their own actions, and consider the security implications of any software installed and configured

Various security issues, such as users not taking care of their credentials, or using unmaintained or unpatched software can have a big impact on EGI as well as on other users.

The EGI Security Policy Group (SPG) provides policies that define the expected behaviour of sites and users to ensure a secure infrastructure. [R 1]

1.3.2 Software development, selection and deployment

In particular, we ask all those who develop, select or deploy software for use on the infrastructure, to consider how secure the software is. To help, we provide a simple checklist of points which should be considered. See section 2.

1.3.3 Carry out vulnerability issue handling according to procedure

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

1.4 SVG, Software Providers, and Scope of SVG.

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

For any organisation providing software with which EGI has an SLA it is compulsory to co-operate with the EGI SVG when potential vulnerabilities are found.

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

For other software, such as VO specific software, SVG provides a checklist in section 2 and handles vulnerabilities as described in this document. Those selecting or deploying the software take the prime responsibility in this case.

1.5 SVG as the 'main handler' of the vulnerabilities for software

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. If SVG is the main handler SVG investigates, contacts the software 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.

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, where EGI is only one of a number of infrastructures using the software, the software 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 software providers are in-between, are aware of SVG but have their own handling procedure. Generally SVG has 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. Since 2015 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, or the '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

SVG cannot guarantee that something important will not 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.

SVG is working on a best-effort basis, but tries to respond as soon as possible, typically within a few hours, giving higher priority to vulnerabilities that appear more urgent. 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 not an SVG task to trawl CVE's, looking for ones that may be relevant.

1.8 Procedure on wiki

A summary of the SVG issue handling procedure is available on the EGI public wiki.

This document does not describe the specific tools used for handling vulnerabilities. Note also that details such as contact information and templates for handling vulnerabilities are not in this document.

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 develops, selects or deploys software which is used on the EGI infrastructure, or think that certain software 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.

Updates and improvements may be made to the wiki version, without revising this document [R 8]

2.1 Who is the Software Provider?

If the Software Provider is an organisation or company, with a record for providing reliable, secure software, then this is a good indicator that the software can be considered for use.

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

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

If the software comes from a reliable software provider, then sections 2.2 through 2.10 will need less consideration.

If the software comes from unknown, small companies or 'hobby' programmers, then sections 2.2 through 2.10 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 professional?

If the software has not been produced by a reliable company or organisation then take a look at it. Does it look good, clear, and professional? Is the code well documented, does it explain clearly what it is doing? Does it compile cleanly, without warnings? Is it the code flow easy to understand? For the more experienced, are there any security issues such as ignoring errors and return codes?

None of these are any guarantee that the software is secure, but indicate that some time has been spent on putting it together in an organized way.

For more information, see [R 9]. SVG has some additional references for secure coding [R 10]

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 contain constructs which may be exploited if user input is not sanitized.

2.5 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 reliable company then it is likely to be adequate.

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 is likely to be supported.

If the software support is no longer funded but there is some party committed to providing updates for at least a year or so, (this should be captured in the form of a MoU) then one can rely on this.

If it is not supported, or relies on someone maintaining it as a hobby then think again about whether security support is adequate.

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.

Have you considered what would be the impact if the software were no longer to be supported in the future?

2.6 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.

2.7 How are software vulnerabilities reported?

It is essential that a new vulnerability can be reported to the software provider, without generating a publicly readable ticket or other publicly available information.

2.8 What are the configuration issues related to security?

Ensure that the software can be configured securely in the circumstances in which you wish to use it. Ideally, the default configuration should be secure. If not, e.g. if there is a default password, ensure that you understand how to configure it securely and if you are suggesting to others that they use this software, include instructions on what needs to be done to configure it securely.

2.9 Does usage of the software comply with the EGI policy on the processing of personal data?

It is important that all activities comply with the EGI Policy on the processing of personal data [R 7]

This policy aims to ensure that data collected as a result of the use of the Infrastructure is processed fairly and lawfully by Infrastructure participants. Some of this data, for example that relating to user registration, monitoring and accounting contains “personal data” as defined by the European Union (EU). The collection and processing of personal data is subject to restrictions aimed at protecting the privacy of individuals.

It must be possible to configure the software such that it complies with this policy.

3 Vulnerability issue handling procedure

The Issue handling is carried out by the SVG-RAT. See section 11.3

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 to report any vulnerability which is discovered in any software that is used on or is relevant to the EGI infrastructure. This includes alerting SVG to vulnerabilities announced by the software providers. For more details see section 4.2

3.1.2 Investigating a vulnerability

The RAT, along with the reporter (if applicable), and the software provider (if appropriate) and any other appropriate party investigate the issue. If it is found to be valid the relevance and effect in EGI are 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 fixing 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 the issue is assessed as 'High' or 'Critical' risk
- 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 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 put in CC. See section 11.5 for more info on where to send advisories.
All vulnerabilities concerning Operating systems should additionally be sent to the VM endorsers. (Note that a suitable mailing list is not yet available, Fed Cloud members who are in the RAT should try to ensure images are updated.)
If the advisory concerns software which is only relevant to EGI Federated Cloud sites, the advisory may be sent to cloud-sites-security-contacts@mailman.egi.eu instead of site-security-contacts@mailman.egi.eu
We plan to have an additional e-mail list which anyone can subscribe to, to which we distribute all advisories and information which is TLP:WHITE.

- For 'High' and 'Critical' vulnerabilities which are NOT already publicly disclosed the advisory is sent as TLP:AMBER See [R 2]
    - It is made public at least 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 it is sent as TLP:WHITE, and placed straight on the 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 11.4

3.3.1 Contact software provider

Contact the software provider and ask 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 TLP:AMBER for 'High' risk vulnerabilities.

The advisory will normally be released as TLP: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 TLP: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.

3.4 Issues where the risk is hard to determine

(Added June 2017)

In some cases, due to the reduced homogeneity of the EGI infrastructure, it is difficult to determine the risk resulting from a vulnerability. It may depend on site specific configuration, or the SVG may simply not have enough knowledge or information to accurately determine the risk or even whether it is possible to exploit a vulnerability in the EGI infrastructure.

If we think in some configurations in EGI the risk is 'High', an advisory may be sent as 'Up to High risk' and suggest sites update.

If we do not know the risk, we may send an 'Alert' rather than an advisory, suggesting sites should look at whether this is relevant to them, and invite them to provide feedback. This informs sites of the issue, as well as indicating that we are aware of it.

In some cases a vulnerability may be widely discussed in the media, but it is of low risk or not exploitable in EGI. In this case we send an 'Information' e-mail.

3.5 Configuration related issues

(Added June 2017)

On a couple of occasions we have found that a security problem exists due to configuration problems. In this case we may ask sites to check the configuration, and take action if necessary. This may be done either as an SVG or IRTF action.

3.6 Notifications to sites

EGI SVG may send 4 types of e-mail:--

- HEADS UP – Sites may be asked to do something urgently soon.
    - Usually only sent for vulnerabilities which may be assessed as 'Critical'
- ADVISORY – Sites instructed to do something
    - The commonest type of mail, e.g. update when vulnerability fixed in software
- ALERT – Sites should be aware
    - This may be important to you, you may want to take action
- INFORMATION – to inform sites of something
    - If a well talked about vulnerability is not relevant
    - Anything else we want to inform sites about

In all cases, we should remember that the mail goes to 300+ sites, and some set off alarms for people on-call so it is important to consider carefully if and when e-mails are sent.

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.

4.2 Reporting a vulnerability

If an EGI user or other person who participates in 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. Additionally, it may be reported via the means (if any) defined by the software provider (see section 2.9). If this additional reporting to the software provider has not been 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 software provider, who, and by what means.

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 11.3)

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

4.3 Reporter may help with investigation

It is very useful 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 private.

The SVG co-ordinator ensures that these activities are carried out.

5.1 When a potential vulnerability issue has been reported

When a potential vulnerability issue has been reported the SVG co-ordinator should do the following:

- Acknowledge the reporter
- Contact the developers or software provider with appropriate information, unless
  - The report is clearly invalid or
  - The software 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 its potential effect. It is important that the software provider is involved in this.

All vulnerabilities should be investigated to understand the likely effect on the 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 12 12 ‘dealing with special 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, to ensure that only the RAT sees the discussion before it has concluded. It should not be held in the tracker entry, as other relevant parties including the reporter may be able to view the discussion. A summary of the reasons for the risk category chosen should be placed in the tracker entry after the risk has been assessed.

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 Software Provider of the outcome

If a TD is set, inform the software 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 software provider 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 they 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 software, 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 software, or is in contact with the software provider, 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 software provider’s 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 put in CC.
For vulnerabilities which only concern EGI Federated Cloud sites, mail may be sent to Cloud-site-security-contacts@mailman.egi.eu instead of site-security-contacts@mailman.egi.eu
In addition, we plan to have a mailing list which anyone can subscribe to and is put in CC for TLP:WHITE information.
For issues announced concerning Operating System distributions, this should additionally include VA/VM Owners and VA/VM Endorsers. Possibly also VM Operators. See section 11.5. At present (June 2017) the exact lists and where they go to are still in discussion.

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

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 some 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 Software Providers and people installing software

SVG should attempt to engage where possible with Software 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 software providers 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 Reporting on the EGI SVG activity

EGI should report on the EGI SVG activity to management when requested. This may include for example statistics on the number of issues handled.

6 Details for Software Providers

Software providers are anyone providing software which has an impact on the EGI infrastructure.

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

Some software providers are specifically writing software for use on the EGI infrastructure and other similar infrastructures. They are aware of SVG, EGI may have an SLA with many of them, and for many of them 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 software provider, and the persons who maintain software in the EGI UMD and CMD as software providers.

VM Endorsers may also be seen as software providers, see section 10.1.

6.1 Ensure up to date information on contact details are 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 software providers with which we have an SLA), or informing SVG of a security mailing list.

6.2 Software Provider and sensitive information

While EGI is increasingly deploying software which is produced by software providers with which we have no direct relationship, there is still software deployed on the infrastructure from providers with which EGI collaborates.

It is not helpful if people can browse either a bug tracker or a version control system and find information on vulnerabilities. Stating something like 'Fix for vulnerability/exploit' in a version control system may alert malicious persons to a problem and help them find and abuse it.

It is best that there is no reference to a vulnerability fix in any public bug tracker or version control system.

The software provider should take care not to disclose information that may be useful for attackers.

6.3 Be ready to investigate a potential vulnerability when reported

If a potential vulnerability is reported the software provider 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 software provider will be increasingly relied upon to establish what (if any) is the problem with the software.

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. The software provider should review this and comment on accuracy and anything else they wish.

6.6 If the Software Provider finds a vulnerability

It is quite common that the software provider finds a vulnerability in their own software, and is able to fix it in a timely manner. It is important that software providers do take action concerning vulnerabilities they find themselves, and don't just ignore them while nobody has complained yet. Software providers 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 described in sections 6.6.1 and 6.6.2.

6.6.1 Software provider informs SVG as soon as the vulnerability is found

This is the preferred option 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 software provider 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 software provider with advice on resolving the issue.

6.6.2 Software provider informs SVG when the vulnerability has been fixed

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

This section underwent a major revision in June 2017.

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 EGI security 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. In 2016 there were 6. The majority concern vulnerabilities in software where the software provider is a large organisation, and the vulnerability is 'announced' having been resolved, or discussed publicly then resolved fairly quickly by the software provider. It is then up to SVG to produce an appropriate advisory for sites, then CSIRT/IRTF to monitor for vulnerable sites. Sometimes information on a vulnerability is made public without having been resolved, these are known as 'zero day' vulnerabilities, and have to be dealt with as appropriate.

In many cases the following 'steps' are carried out in parallel. These should be seen as steps that should be considered, some will be more relevant than others in each case, and some may be skipped if it is deemed urgent to get the advisory out to protect the infrastructure. Most will only be relevant if the critical vulnerability has not already been resolved.

Note that up to now 'Critical' vulnerabilities where there isn't a fix immediately available have been quite rare, less than 1 per year.

7.1 Consider whether to alert management

If a vulnerability is in software which is widely used, and on which EGI heavily depends, it may be appropriate to alert management.

Alerting management may be done at any stage, if it is considered useful and not necessarily at the beginning.

7.2 Alert all appropriate parties

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

7.3 Consider having a teleconference call to discuss the options

It may be useful to have a teleconference call between the RAT members, IRTF members (who are in the RAT anyway) and others. This may help speed up the risk assessment and possible mitigation strategies, particularly when communication via e-mail did not lead to consensus.

Any appropriate people may be invited. This may include the development team (in the case where EGI is the main user of this software, EGI SVG the main handler of vulnerabilities), and possibly management.

7.4 Actions should be agreed before being carried out

It is not usually necessary to take action in a matter of minutes. Any action taken, e.g. informing sites, asking them to take action should be agreed by a number of people. This should include the EGI security officer on duty.

This does not change the fact that the security officer on duty or the EGI Security officer or the IRTF chair may take any action they wish, but this is not an SVG action.

7.5 Consider sending a 'heads up' to sites

This is an alert to sites that a potentially 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 software 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.

This may be sent by SVG or IRTF. In the case where a problem affects only a minority of sites, it may be more appropriate for IRTF rather than SVG to send the 'Heads up', as IRTF have tools to send to a subset of sites running specific software.

7.6 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 an exploit is not possible or extremely unlikely under our circumstances.

This task may be delegated to one or two individuals with the appropriate skills and knowledge.

7.7 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 would take longer.

7.8 Decide whether to wait for a patch

Decide whether to wait for a patch, or whether to recommend other action. Note that this may be carried out in conjunction with 7.9

7.9 Find if any action can mitigate or resolve the problem

Consider whether any mitigating action can be recommended. If so consider drafting an appropriate advisory and sending that to recommend the mitigating action.

7.10 Consider asking management

If there is more than one option, for example one option may be to wait a few days and take the risk, another may be to take action which severely impacts the availability of the EGI infrastructure, asking management's opinion may be a sensible option and normally this query should include a recommendation.

In the case where the recommended option impacts service availability, management should also be requested to ensure that sites are not penalized via availability statistics if they carry out the recommended action.

7.11 Send Advisory if sites are recommended to take action before a patch is available

Draft and send an advisory/alert if sites are being recommended to take action before the patch is available. This may be mitigating action, or it may be a recommendation to stop using the software. This may be carried out either by IRTF or by SVG. In the case where a problem affects only a minority of sites, it may be appropriate for IRTF rather than SVG to send, as IRTF have tools to send to a subset of sites running specific software.

7.12 Draft Advisory

Ensure the advisory is completed prior to the software release. This may require a few small changes before distribution, such as date and version number, but it should be as close as possible to being ready to send.

7.13 Release advisory

SVG should send the advisory as in 3.1.6 when the vulnerability is fixed.

If the vulnerability is not public send as TLP:AMBER and release publicly no less than 2 weeks later.

7.14 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 software provider is the VO, and the VO has the same responsibilities as any other software 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 Cloud and Virtualization enabling software

(New June 2017)

9.1 OpenStack and OpenNebula

These are treated in the same way as the Linux operating system, and any other 3rd party software widely used in the EGI environment.

9.2 Hypervisors

These are treated in the same way as any other 3rd party software.

9.3 EGI Cloud Middleware Distribution- CMD

Some of the tools used to enable the EGI Federated Cloud, which act on top of OpenStack and OpenNebula, are distributed in the EGI CMD. Such software will be treated in the same way as software in the EGI UMD or CMD, where EGI SVG may be seen as the 'Main handler' of software vulnerabilities as in 1.5.

9.4 E-mail contact for EGI Federated Cloud sites

An e-mail list has been produced which allows us to contact only sites which provide services to the EGI Federated Cloud. This is Cloud-sites-security-contacts @mailman.egi.eu

10 Virtual Machines and Vulnerabilities

Note June 2017 – some more information added, but still some points need to be resolved.

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 following 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.

10.1 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.

The VM image or Virtual Appliance must be based on a fully-patched operating system image, and it is the VM endorser's responsibility to ensure that the image is kept up to date and in particular updated to eliminate any software vulnerabilities considered 'Critical' or 'High' risk.

An endorsed VM image containing vulnerable software is seen like a vulnerability, the endorser being the software provider, if it is a case of either:

- being misconfigured (e.g. containing passwords, private keys etc.) or
- including vulnerable non-standard, poorly maintained software.

In such cases 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' or '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 VM images 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.) (Note June 2017, not yet got a VM endorser list.)

10.2 VM Operator and vulnerabilities

VM Operators are responsible as in [R 3].

VM Operators should only run endorsed VM images.

If a VM Operator adds software at the time of 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' or 'Critical' by SVG it is planned that VM Operators should receive the advisories issued by SVG. It should be noted that VM Operators 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.

10.3 VM Operators authorization and contact

In order to be able to operate VMs in the EGI Federated Cloud, VOs need to give members the VM Operator role. This is now enforced in the AppDB. At present, most of the VOs that are supported in the Federated Cloud have the VM Operator role assigned to all their members.

SVG would like to have a VM Operator contact list, but how this is provided is uncertain.

11 Descriptions and explanations

11.1 What is a vulnerability?

There are many definitions of a software vulnerability. We usually consider a vulnerability as a problem where an individual or group can gain access to or influence the behaviour of 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 consider appropriate.

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

11.2 What is NOT a vulnerability?

11.2.1 Actions that can only be carried out by site administrators

In general, site administrators essentially are trusted at the sites they manage – and they are assumed to be able to access and manipulate data stored on their equipment. The only things that they are not trusted with are decryption keys for encrypted data. 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.

11.2.2 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. For example, a segmentation fault may reveal information that a given deployment might in principle be vulnerable to some specially crafted attack. These can again be rejected, treated as standard bugs or as vulnerabilities as the RAT considers appropriate.

11.2.3 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.

11.3 The 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, NGI representatives and experienced site administrators. 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 vulnerability reported and allows them to provide their opinion or comment on any issue they wish.

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. This includes making sure that contact details for the developers are available, the infrastructure is in place, and the various parts of the process are carried out in a timely manner.

11.4Adjusted 'responsible disclosure'

The SVG has always followed a procedure for 'responsible disclosure' which helps to encourage the reporting of vulnerabilities to our group.

In the past this meant that any advisory would be made public shortly after the corresponding vulnerability was fixed (allowing some time for affected parties to update their systems), or else on the Target Date, whichever was the sooner. In the course of time, however, it became clear that disclosing issues on the Target Date if they are not fixed may not always be in the best interest of EGI as a whole. We therefore have adjusted the procedure so that now for 'High' and 'Critical' risk vulnerabilities, once the Target Date has passed and the vulnerability is not yet public, the advisory is sent with classification 'TLP:AMBER'.

It then remains 'TLP:AMBER' until at least 2 weeks after the issue is fully resolved.

11.5 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 and any other recipients deemed relevant by the RAT.

It is better that people have to ignore a vulnerability which is not relevant to them, than not to receive information on a vulnerability which is relevant to them.

There is a list for sites deploying cloud services which may be used for vulnerabilities concerning cloud enabling software or hypervisors. It is cloud-sites-security-contacts@mailman.egi.eu

For advisories concerning Linux or other commonly used software, in addition advisories should go to VM Operator contacts and VM Endorser contacts (at time of writing, not yet available).

12 Dealing with special 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 be very complex to try to define every possible situation.

12.1 Be aware of the purpose of the group.

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

12.2 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 information allowing a third party to associate jobs or data with DNs, which is against data protection legislation.

12.3 Issues 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 software is affected or how. In this case it makes sense to contact those software providers for which EGI is the ‘main handler’ (section 1.5) of vulnerabilities concerning their software. For now, the ‘URT discuss’ list will be informed. In future, a more comprehensive list may be available.

13 Notes on Risk

13.1 Risk Categories

Some guidelines on risk categories are on the SVG wiki, entitled ‘Notes on Risk’. [R 6]

Note that this is under revision.

13.2 Risk is the judgement of the RAT

This has always been the case, and remains so. There are no hard rules on risk, and specific factors in EGI may increase or reduce the risk, according to how software is used in a large shared distributed infrastructure.

For example, if a vulnerability is public and there is a public exploit, then this is likely to be of higher risk than a vulnerability that is not public, even if the impact is the same.

13.3 Critical/High Boundary

We have made a very small change in where we consider the boundary between ‘High’ and ‘Critical’ to be.

From now on if SVG/IRTF cannot find an exploit which is likely to work in EGI, even if the impact were to be serious, the vulnerability will be assessed as ‘High’ with a warning that it is likely to be elevated to ‘Critical’ if an exploit is found.

For some cases where the vulnerability has been reported to us, and is not public, and is both difficult to find and exploit, and the software is produced by our collaborators where we can have some influence on the distribution of the software, a vulnerability may be considered ‘High’ rather than ‘Critical’ even when the potential effect of the exploit is serious. In this case we will wait at least 4 weeks rather than 2 after it has been fixed and sites have been asked to upgrade, before placing the advisory on the wiki. Additionally, we will ask all distributions to update or remove the vulnerable software before the advisory is placed on the wiki. Of course, there will be a similar warning that this may be elevated to ‘Critical’ if more information or an exploit is released publicly.

14 Software and vulnerabilities

This table indicates 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 software providers

Software Source	***Software Provider aware or vulnerability announced***	***Software Provider not clearly aware of vulnerability***	***Risk Assess***	***Advisory Issued***	***Comments***
EGI UMD, CMD and 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 software provider	Software provider should co-operate with SVG	Inform Software Provider	Yes	Usually all valid vulnerabilities	
Other software widely installed on EGI infrastructure	Usually the case	Inform Software Provider	Yes	Usually only if assessed as 'Critical' or 'High'	Mostly this concerns 'announced' vulnerabilities. Common situation.
VO specific S/W	Also usually handle according to this procedure	Inform Software Provider	Yes	Usually	
Software not installed on the EGI infrastructure	No action after establishing it is not relevant to EGI	Simply forward info to Software Provider	No Risk due to being irrelevant	No	Unlikely such vulnerabilities are reported to us

15 References

No	Description/Link
R 1	The EGI Security Policy Group https://wiki.egi.eu/wiki/SPG
R 2	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
R 6	Notes on Risk https://wiki.egi.eu/wiki/SVG:Notes_On_Risk
R 7	EGI Policy on the processing of Personal Data https://documents.egi.eu/public/ShowDocument?docid=2732
R 8	Software checklist on SVG Wiki https://wiki.egi.eu/wiki/SVG:Software_Security_Checklist
R 9	Good coding practices https://www.mir-swamp.org/
R 10	Secure coding on SVG wiki https://wiki.egi.eu/wiki/SVG:Secure_Coding