EGI Software Vulnerability Group (SVG)
Software Vulnerability Handling Procedure

Author: Linda Cornwall and the EGI SVG

Version: 0.11 for EGI ACE

Document Link: **https://documents.egi.eu/document/3867**

This work by EGI.eu is licensed under a
Creative Commons Attribution 4.0 International License

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
v.0.1	10/01/2022	First Draft for EGI ACE	Linda Cornwall
V 0.2	12/01/2022	Some mods including adding NDA's to appendix Changes to Moderate and Low	Linda Cornwall
V 0.3	18/01/2022	Changes after discussion with CSIRT virtual F2F Mainly changes to scope, Limitations statement, and more changes to Moderate and Low risk vulnerabilities	Linda Cornwall
V 0.4	8/02/2022	Introduction of new 'Critical – Emergency' Added a section on risk generally Same non-disclosure agreement for DEG and RAT. Some minor tidying of grammar	Linda Cornwall
V 0.5	04/03/2022	Removed details on risk – I think this should be somewhere else.	Linda Cornwall
V 0.6	26/04/2022	Very minor change to NDA to state info learnt through participation in SVG	Linda Cornwall
V 0.7	27/04/2022	Change in section 2.2.3 to send info to operations@egi.eu	Linda Cornwall
V 0.8	16/06/2022	Change to simplify and speed up public vulnerabilities which are in scope and critical risk	Linda Cornwall
V 0.10	21/06/2022	Small changes from Pinja and Baptiste's comments	Linda Cornwall
V 0.11	27/07/2022	Very minor change to section 3.1 to say aim to have a RAT member on duty, plus get more active RAT members.	Linda Cornwall

TERMINOLOGY

The EGI glossary of terms is available at: https://ims.egi.eu/display/EGIG/

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 http://repository.egi.eu/
CSIRT	(The EGI) Computer Security Incident Response Team	Responsible for operational security in EGI

CVE	Common Vulnerabilities and Exposures	A dictionary of common names (i.e., CVE Identifiers) for publicly known cyber security vulnerabilities
DEG	Deployment Expert Group	Group of volunteers who help handle vulnerabilities for which they have the appropriate knowledge, this enables us to expand the knowledge to handle the wider variety of software used in the EGI infrastructure
iRAT	issue Risk Assessment Team	Team which handles a specific vulnerability, comprising of RAT members, DEG members, and others appropriate for handling the particular vulnerability.
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://confluence.egi.eu/display/EGIG/Traffic+Light+Protocol
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 7
1.1 Purpose of this document 7
1.2 Reason for revision 7
1.3 OMB Approval 7
1.4 This is the 'definitive' version of the procedure 8
1.5 Technology neutral 8
2 Purpose, Scope and Limitations Statement 9
2.1 Purpose of the EGI SVG 9
2.2 Scope of the EGI SVG 9
2.2.1 Software in the EGI repository 9
2.2.2 Other Software deployed on the EGI infrastructure 9
2.2.3 Software used for centrally operated services 9
2.2.4 EOSC services – generally NOT included 10
2.3 Limitations Statement 10
3 Groups and functions 11
3.1 Software Vulnerability Group (SVG) Risk Assessment Team (RAT) 11
3.2 Deployment Expert Group (DEG) 11
3.2.1 Look out for and report vulnerabilities in software you use 11
3.2.2 Respond when asked if an issue is 'In Scope' 12
3.2.3 Volunteer for the iRAT if you have expertise 12
3.3 Issue RAT or iRAT 12
3.4 EGI CSIRT 12
4 Software Vulnerability Handling Procedure 13
4.1 Determine whether it is a software vulnerability 13
4.2 Is the vulnerability publicly announced and not obviously out of scope? 13
4.2.1 Initial request to SVG RAT and DEG 13
4.2.2 Acknowledge and communicate with reporter 14
4.2.3 In parallel, draft advisory 14
4.2.4 Update advisory if necessary, according to the responses 14

4.2.5 Decide whether to send advisory with information available 14
4.2.6 Is detailed investigation necessary? 14
4.3 Ensure the software provider is aware of the vulnerability 14
4.4 If it is a software vulnerability, determine scope 15
4.5 Form the iRAT 15
4.5.1 Who is in the iRAT? 15
4.5.2 Sub-procedure for forming the iRAT 15
4.5.3 How many iRAT members is considered sufficient? 16
4.6 Engage with reporter, various peers, determine if Embargo is in place 16
4.6.1 Acknowledge and communicate with reporter 16
4.6.2 Engage with peer infrastructures with whom we collaborate 16
4.6.3 Determine if embargo is in place 16
4.7 iRAT investigates the vulnerability 16
4.8 iRAT and SVG-RAT - Carry out risk assessment 17
4.9 SVG-RAT - Set Target Date and inform the software providers 17
4.9.1 Set target date for resolution 17
4.9.2 Inform software providers and distributers of Risk and Target date 17
4.10 iRAT and SVG-RAT Identify what action is to be taken by whom. 18
4.11 SVG-RAT – Is the issue fixed? 18
4.11.1 Yes 18
4.11.2 No 18
4.12 Is there any embargo on the information? 18
4.13 Inform appropriate parties of action to be taken 19
4.14 Are all actions from SVG completed? 19
4.14.1 If interim or incomplete advice given 19
4.14.2 If advisory/information sent as [AMBER] 19
4.14.3 If no further action is envisaged concerning this ticket 19
5 Details on some actions 20
5.1 ProcedureEnd 20
5.2 Risk Categories 20
5.2.1 Critical Risk 20

5.2.2 High Risk 21
5.2.3 Moderate Risk 21
5.2.4 Low Risk 21
5.3 Vulnerabilities assessed as Critical risk 21
5.3.1 Consider whether to alert management 22
5.3.2 Alert all appropriate parties 22
5.3.3 Consider having an on-line conference to discuss the issue 22
5.3.4 Actions recommended by SVG should be agreed before being carried out 22
5.3.5 Consider sending a 'heads up' to sites 22
5.3.6 Find out how quickly a patch can be made available 23
5.3.7 Decide whether to wait for a patch 23
5.4 Advisories and other notifications 23
5.4.1 Types of e-mail sent 23
5.4.2 Traffic Light Protocol 23
5.4.3 Moderate and Low risk vulnerabilities 24
5.4.4 Where to send 24
6 NDA for joining both the RAT the DEG 26
7 References 27

1 Introduction

The purpose of the EGI SVG is “To minimize the risk of security incidents due to software vulnerabilities”

The EGI SVG is NOT trying to substitute/compete with various other vulnerability activities external to EGI.

The EGI Software Vulnerability Group (SVG) and its predecessors has been handling software vulnerabilities since 2005, having clear procedure in 2006 (EGEE-II) with relatively minor changes since including: --

- Going from being focused on Grid Middleware to all types of software on the EGI distributed infrastructure
- SVG handling vulnerabilities in software produced to enable services, which EGI endorses e.g., in UMD/CMD

The previous document “EGI Strategy and Vulnerability Issue Handling Procedure” [R 1] described this procedure approved in 2017 concerning Software vulnerability handling

1.1 Purpose of this document

This document defines the procedure for handling software vulnerabilities reported to the EGI software vulnerability Group and will replace [R 1] concerning the procedure for handling software vulnerabilities.

This document also confines itself to software vulnerability handling and does not include other activities which help fulfil the purpose of the EGI SVG, such as a checklist for the selection and deployment of software.

1.2 Reason for revision

This document replaces the previous document “EGI Strategy and Vulnerability Issue Handling Procedure” [R 1]. The procedure described in this previous document worked well when we had a relatively homogenous environment, but in recent years the environment has become less homogenous, with a proliferation of software in use, and a change of strategy and procedure is needed.

1.3 OMB Approval

EGI SVG will seek approval by the EGI Operations Management Board (OMB). This is effectively permission/agreement on what we do, the limitations, and the procedure. For example, this helps cover us in case someone complains if a vulnerability is exploited while we are waiting for a fix and says, ‘Why didn’t you tell us about it?’ This also covers caveats in the limitations of what the EGI SVG can do.

OMB approval is also needed so that sites may disrupt services to secure themselves in case of being asked to take action to address a 'Critical-Emergency' vulnerability.

1.4 This is the 'definitive' version of the procedure

This is the version of the procedure which we have agreed, after approval by the EGI OMB. A summary will be placed on the EGI web pages (currently confluence).

1.5 Technology neutral

This is described in a way which is as technology neutral as possible.

Details related to any specific technology which is currently being used, will be placed on the web.

2 Purpose, Scope and Limitations Statement

2.1 Purpose of the EGI SVG

The purpose of the EGI SVG is “To minimize the risk of security incidents due to software vulnerabilities”. Our aim is to help sites avoid being exposed to software vulnerabilities, including via a procedure for handling vulnerabilities reported to the EGI SVG which this document describes.

2.2 Scope of the EGI SVG

This document attempts to describe our procedure for handling software vulnerabilities in a manner that is scope neutral. However, here we explain the scope of the vulnerabilities we plan to handle in detail according to this procedure, at least initially. This may be expanded later.

The scope for DETAILED Issue handling is as follows: --

2.2.1 Software in the EGI repository

The main scope of EGI is Software in the EGI repository [R 2]

This software is effectively approved and distributed by EGI to enable the sharing of computing resources.

This consist of the Unified Middleware Distribution (UMD) and the Cloud Middleware Distribution (CMD).

This will include the new AAI, token software which is expected to be in the UMD.

2.2.2 Other Software deployed on the EGI infrastructure

Other Software deployed on the EGI infrastructure and EGI services [R 3] is handled on a ‘best efforts’ basis.

This includes relevant Linux OS distributions, Software we know are deployed on the infrastructure e.g. HTCondor and Singularity, which will normally be handled by the EGI SVG, but this is not guaranteed.

Other software which is deployed on multiple sites may be handled – but scope is dependent on participation of suitable experts in the Deployment Expert Group (DEG) 3.2.

2.2.3 Software used for centrally operated services

For centrally operated services on which EGI depends, no detailed analysis or risk assessment needs to be carried out. A simple e-mail to operations@egi.eu should be sent, to ensure that they are aware of the vulnerability.

The operations group along with EGI IT support group will normally simply keep services up to date, without any dependency on the EGI software vulnerability group.

2.2.4 EOSC services – generally NOT included

The initial focus is on EGI, even though EGI ACE is advanced computing for EOSC.

Previously we planned to include the EOSC hub portfolio [R 4], although we will include appropriate AAI which is also used for EGI initially we will not include this or its successor. This may be included later if we get appropriate participation in the Deployment Expert Group (DEG).

The 300+ services in the EOSC marketplace [R 5] are NOT included for detailed vulnerability handling. The main strategy is to suggest how they are handled via good practice as advised in the newly formed WISE working Group 'Best Practices for handling Software Vulnerabilities' [R 6].

2.3 Limitations Statement

The EGI Software Vulnerability Group (SVG) does not guarantee its work in any way, including that SVG will handle vulnerabilities correctly or have the resources to handle all vulnerabilities reported.

We will do our best to fulfil our purpose "To minimize the risk of security incidents due to software vulnerabilities". All work carried out by the EGI SVG is done on a best-efforts basis.

The EGI Software Vulnerability Group (SVG) does not attempt to replace other vulnerability handling activities in the wider world. Service administrators and site security contacts are themselves the first line of defence for their own sites, and responsible for the site security.

Various other forums publish advisories, and EGI CSIRT / SVG will by default not resend any advisories published on such forums. The SVG is mainly concerned with specific software that is widely used to enable distributed computing for EGI communities, and the security risks related to how it is used in EGI.

SVG does not generally handle software vulnerabilities outside its scope. In exceptional cases SVG/CSIRT may post information when a public vulnerability is considered 'Critical' even if it is outside our scope.

We emphasise that SVG does not guarantee that all software vulnerabilities in scope are handled. We may not know about them, or we may not have the resources to handle them. SVG does not guarantee that the vulnerability handling is correct: in cases where we assess the risk it is the opinion of the group assessing the risk, based on the best of knowledge of how the software is used in our infrastructure.

We also note again that our ability to operate is dependent on participation from relevant experts and other parties.

3 Groups and functions

This describes the main groups and functions which interact with the EGI SVG and the procedure.

3.1 Software Vulnerability Group (SVG) Risk Assessment Team (RAT)

This is the main group of people who carry out the software vulnerability handling process. This includes: --

- Defining the procedure
- Getting the procedure approved by the OMB
- Configuring the ticket handling
- Managing any other tools needed, including web pages
- Carrying out the handling of vulnerabilities according to the agreed procedure, with input from various other groups.

This group has been running the vulnerability handling for more than a decade and will continue to do so.

When joining, members are asked to reply by e-mail to a simple non-disclosure statement with 'I agree'. See 6

One member of the RAT should be available/on duty on each working day. A Rota will be kept on the SVG private website. We note that this may not be possible at all times, but it is our aim and we will attempt to get more active RAT members if possible.

3.2 Deployment Expert Group (DEG)

This is a group of people who are invited to help us cope with the increased inhomogeneity of the EGI infrastructure. These people are experts in software deployed on the EGI infrastructure, select software for deployment on the EGI infrastructure, and consider how software is configured.

When joining, members are asked to reply by e-mail to a simple non-disclosure statement with 'I agree'. See 6

Members of the Deployment Expert Group are asked to do 3 things: --

3.2.1 Look out for and report vulnerabilities in software you use

It is important that DEG members are alert to software vulnerabilities announced by the providers of software they deploy, and report via report-vulnerability@egi.eu any they consider serious and relevant to EGI.

In addition, vulnerabilities DEG members discover themselves should also be reported via report-vulnerability@egi.eu.

One may of course also report them to the software provider, if able to do so without exposing the vulnerability publicly. Alternatively, SVG will be happy to handle that for you.

3.2.2 Respond when asked if an issue is 'In Scope'

Sometimes when a vulnerability is reported, SVG-RAT members are not aware of whether the software is used in the EGI infrastructure

Please respond to this question, particularly if you use the software.

If there is no response confirming an issue is in scope, it typically implies we will not look further into it. If there was agreement that the issue should indeed be out of scope, it can be labelled as such. If there was no conclusion (for example due to lack of response), we should indicate that fact instead.

Note that Scope depends on participation.

3.2.3 Volunteer for the iRAT if you have expertise

If an issue has been decided to be 'In Scope', we will ask for volunteers to join the iRAT. 3.3

This is probably the most important function of the DEG, to find the appropriate members of the iRAT for a particular issue.

Investigating the impact of vulnerabilities depends on getting appropriate members of the iRAT to look at the issue and its effect according to how software is deployed.

3.3 Issue RAT or iRAT

This is the group of people who investigate a particular software vulnerability issue. It is composed of SVG RAT members, members of the DEG who volunteer because they have knowledge of a particular issue, sometimes it will include the reporter of the issue if appropriate, sometimes the software developer(s), and any other people who it is appropriate to include for a specific issue.

3.4 EGI CSIRT

This is the EGI Computer Security Incident Response Team. At any time, at least during working days one member is the ‘Security Officer on Duty’.

All Members of CSIRT who take the role of ‘Security Officer on Duty’ should be members of the SVG RAT, so that they view all information that the SVG has access to. It should be noted that CSIRT may act in any way it wishes. This may include advising sites to patch or stop using a particular piece of software if they wish.

EGI CSIRT is responsible for ensuring security, EGI SVG advises and assists.

4 Software Vulnerability Handling Procedure

This describes the procedure. This is what should happen most of the time. Sometimes an unusual situation may occur, and we carry out different actions.

To anticipate every possible scenario, is not reasonable or realistic. The SVG-RAT will carry out any actions they consider sensible according to a situation which arises.

Procedure is triggered by the reporting of a vulnerability.

Anyone may report a Software Vulnerability by e-mail to: -

report-vulnerability@egi.eu

This should be used to report any vulnerability which is discovered in any software that is used on or is relevant to the EGI infrastructure. This should also be used to alert SVG to vulnerabilities announced by the software providers which may be relevant to EGI.

Most of the actions are carried out by the SVG-RAT, the iRAT carries most of the investigations of a specific vulnerability, and recommends what actions to take concerning that vulnerability in the EGI environment

4.1 Determine whether it is a software vulnerability

If it is NOT a software vulnerability, but there is another reason to re-route the information such as it is a legitimate security concern re-route it as appropriate.

ProcedureEnd.

4.2 Is the vulnerability publicly announced and not obviously out of scope?

Most software vulnerabilities reported in recent years are publicly announced, rather than vulnerabilities discovered by the reporter. In this case for those which are relevant/in scope for EGI and 'Critical' risk there needs to be a fast process for handling them in the case of vulnerabilities which we consider to be 'Critical' risk. In this case it is often not necessary to carry out detailed investigations, just to establish that it is relevant, inform sites (mainly pointing to public information), and ask them to act usually to apply patches, sometimes to take other mitigating action.

If not go to 4.3

4.2.1 Initial request to SVG RAT and DEG

Ask both SVG RAT and the DEG

- If the vulnerability is in scope

- If there is any reason to elevate or reduce the risk in our environment
- Their opinion on risk to EGI
- Any information or recommendations they think should be in the advisory
- If they think this vulnerability needs more detailed investigation by the SVG
- Anything else they want to say

4.2.2 Acknowledge and communicate with reporter

Acknowledge the reporter and include asking whether s(he) wishes to be credited should an advisory or other information be issued.

Default is no credit to the reporter.

4.2.3 In parallel, draft advisory

Draft the advisory based on public information

Include any useful information from the responses.

Circulate to/or provide access to SVG-RAT and any DEG members who respond.

4.2.4 Update advisory if necessary, according to the responses

The advisory can be updated depending on the responses.

4.2.5 Decide whether to send advisory with information available

If appropriate send the advisory. We aim to send within 48 hours of the initial report for 'critical' vulnerabilities which do not require detailed investigation by SVG, unless it is on a weekend or public holiday.

4.2.6 Is detailed investigation necessary?

If so move to 4.4 – omitting any steps already carried out in this sub-procedure.

Otherwise move to 4.13 or 4.14 as appropriate.

4.3 Ensure the software provider is aware of the vulnerability

If the software provider has announced a vulnerability, the software provider is clearly aware of it.

If it has been 'discovered' by the reporter, then ensure that the software provider has the information on the vulnerability. Sometimes this is necessary when a vulnerability is found by the reporter in software which is written by those we collaborate with.

If it is necessary to inform the software provider, ensure this is done in a way which does not make the vulnerability public.

4.4 If it is a software vulnerability, determine scope

If it is only relevant to EGI centrally operated services on which EGI depends send an e-mail to it-support@egi.eu. ProcedureEnd

If it is obviously in scope for the EGI infrastructure – note that this may include widely used software which may be used by some VOs - continue with next step.

If it is obviously out of scope – ProcedureEnd

If it is not clear, ask DEG members if it is in scope, if there is a positive response continue with next step, if not, ProcedureEnd

4.5 Form the iRAT

The iRAT (or issue RAT) is the group of people who investigate, risk assess and suggest actions concerning this specific vulnerability.

4.5.1 Who is in the iRAT?

All SVG-RAT members will have access to all information on an issue. But there is a need to identify how many of the SVG-RAT members are able and willing to investigate a particular issue.

Software Providers/suppliers, if they are people we know, or collaborate with.

Reporter of the vulnerability

4.5.2 Sub-procedure for forming the iRAT

Identify persons from SVG-RAT who have knowledge on this issue.

Is the reporter suitable and willing? If so add.

Are the software providers able to join in? for example, if we collaborate with them? If so add.

Add any other known suitable contacts to the iRAT for this issue.

Ask DEG for volunteers and add any to iRAT

If there are insufficient iRAT members

Ask SVG-RAT and DEG again for iRAT volunteers

Allow 1 working day day –

Add any new volunteers to iRAT

Endif

If we consider there are sufficient iRAT members (see 4.5.3)

Continue procedure

Else

Handle failure:

- report to management
- possibly send a notification to potentially affected parties
- ProcedureEnd

Endif

4.5.3 How many iRAT members is considered sufficient?

This is partly dependent on the type of issue. It may be that we are happy with one or two persons who we know are competent to carry out the investigation to understand the issue, plus a few SVG-RAT members to do the risk assessment. In some cases we may need more members.

4.6 Engage with reporter, various peers, determine if Embargo is in place

Note these steps may be done in parallel to one another, and the steps in 4.5 and 4.7

4.6.1 Acknowledge and communicate with reporter

Acknowledge the reporter and include asking whether s(he) wishes to be credited should an advisory or other information be issued.

Default is no credit to the reporter.

4.6.2 Engage with peer infrastructures with whom we collaborate

Engage with peer security contacts with whom we collaborate, possibly adding them to the iRAT if appropriate

4.6.3 Determine if embargo is in place

Determine if embargo period is in place, (that is, if information is at least temporarily confidential) determine disclosure date and conditions. Clearly if the information has been announced publicly there is no embargo. Add disclosure date to ticket if appropriate.

4.7 iRAT investigates the vulnerability

In the case where the vulnerability has been discovered by the reporter, particularly if it is in software written by those we collaborate with, then the investigation includes determining if the vulnerability is real. In this case it is important for the software provider to be involved in this investigation.

Regardless of whether the vulnerability is discovered by the reporter (for example if it is in software written by those we collaborate with), or whether it is one publicly announced which we are alerted to, the investigation will also include what the effect is on our infrastructure, including whether it is relevant, what the likely security effect is.

If the issue is not valid or has no impact on anything in scope ProcedureEnd

4.8 iRAT and SVG-RAT - Carry out risk assessment

Assess the risk for this vulnerability.

This may include for example Risk to Service(s), Risk for each Infrastructure, Risk to Confidentiality.

Any iRAT member for this vulnerability plus any SVG-RAT member is encouraged to give their opinion on the risk. The issue is put into one of 4 risk categories 'Critical', 'High', 'Moderate' or 'Low'.

In some cases, with the agreement/request from IRTF, some 'Critical' risk vulnerabilities may have a 'Critical – Emergency' elevated level.

Some more information on risk categories is at 5.2

4.9 SVG-RAT - Set Target Date and inform the software providers

4.9.1 Set target date for resolution

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
- High – 6 weeks
- Moderate – 4 months
- Low – no longer set a Target date

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.

4.9.2 Inform software providers and distributers of Risk and Target date

If the issue is written by our collaborators, then inform them of the risk and target date for resolution. Also inform those who manage the CMD and UMD if the software is available there.

For moderate and low risk issues, ask them to include information on the vulnerability in the release notes.

For High and Critical, ask them not to include details in the release notes immediately they are released, to enable sites to patch after we send the advisory before making the information public.

4.10 iRAT and SVG-RAT Identify what action is to be taken by whom.

Almost always action WILL be recommended for 'Critical' and 'High' risk vulnerabilities.

In most cases, no action will be taken by SVG if the vulnerability is considered 'Moderate' or 'Low' risk, if the vulnerability is announced by a software supplier. Focus will be on 'Critical' and 'High' risk vulnerabilities.

The most common action will be for sites to update to a fixed version of the software when a patch becomes available.

Mitigation may also be recommended, particularly for 'Critical' vulnerabilities if no patch is available.

Draft recommendations on action to be taken.

If the vulnerability has been announced publicly, and a CVSS score has been publicised, include the CVSS score. If we are rating something 'High' or 'Critical' and the CVSS score does not seem high enough to justify this, explain why we are rating it differently – which may be due to the way the software is used in the EGI infrastructure.

Action may be taken by sites, cloud sites, VOs, or others.

For 'Critical' risk vulnerabilities CSIRT requires sites to take action in 7 days, and for 'Critical-Emergency' risk vulnerabilities CSIRT requires sites to take action as quickly as possible, in any case within 3 days.

If no action is to be taken, ProcedureEnd

4.11 SVG-RAT – Is the issue fixed?

4.11.1 Yes

Update the recommended action to include any information on fixed software version.

Carry out final edits of advisory/information.

4.11.2 No

If Critical – consider the suggested actions in section 5.3 and consider which, if any, of these actions need to be carried out.

If not critical, consider whether there is a need to carry out an action now.

If not, wait for the software to be fixed, or target date, whichever comes first.

4.12 Is there any embargo on the information?

If there is wait until the embargo is over.

If appropriate, carry out any discussions with those who impose the embargo conditions, for example those issuing the embargo may not want the information to be public, but are happy to have an [AMBER] advisory, which may allow SVG to proceed to the next step.

4.13 Inform appropriate parties of action to be taken

Has the reporter responded? If so, and requested, credit reporter in the information.

If not? Ask again whether they wish to be credited.

Carry out any further edits needed to the recommended actions.

Most commonly this will be in the form of an Advisory to all sites, cloud sites only, and sometimes VOs.

Often this will be sent as [AMBER] information, and not made public initially.

Other actions may include: --

Inform a particular single installation or small number of installations of a problem.

4.14 Are all actions from SVG completed?

If they are not, then leave the ticket open.

4.14.1 If interim or incomplete advice given

For example, if an advisory was issued to take mitigating action as the issue was not fully fixed it may be necessary to jump back to 4.11

4.14.2 If advisory/information sent as [AMBER]

Wait until the SVG and any other parties agree it should public, usually should wait at least 4 weeks from asking sites to carry out action concerning a vulnerability before making information public.

Make information public.

4.14.3 If no further action is envisaged concerning this ticket

ProcedureEnd.

5 Details on some actions

5.1 ProcedureEnd

Procedure End does not usually mean do nothing, even if detailed handling is not required.

In most cases it at least means informing the reporter of the outcome, even if it it's out of scope for detailed handling and very little action is considered necessary. In the case where the report is SPAM mail to the report-vulnerability list then we do not reply to the reporter.

In some cases, it may mean we do nothing in detail, but put information on a web page on this vulnerability, and why it isn't being handled in detail by SVG.

In some cases, it may mean sending sites and 'informational' 5.4. One example may be if an issue is being talked about a lot in the media, or people within the project are concerned about it, but it is not a serious problem for EGI. It may make sense to inform sites that we have looked, but do not consider it serious.

It will always involve closing the ticket when no further actions are envisaged.

5.2 Risk Categories

We divide into 4 Risk categories: Critical, High, Moderate and Low.

The basic guidance for the categories is as follows.

5.2.1 Critical Risk

Usually, there is a substantial risk that a vulnerability will be exploited in the short-term, in a matter of days. Examples include: --

- An anonymous or unauthorised user can gain root or admin access
- An anonymous or unauthorised user can carry out widespread damage, data destruction or access to confidential data
- A public exploit is available allowing an authorised user to gain root or admin access
- A public exploit is available allowing unauthorised access
- Most cases of identity theft and impersonation

In some cases, if the exploit is public and trivial to exploit, the vulnerability may be considered 'Critical – Emergency'. This is where sites exposing this vulnerability are likely to be in immediate danger of compromise. Sites should

For 'Critical' risk vulnerabilities sites are expected to act within 7 days or face site suspension.

For 'Critical-Emergency' risk vulnerabilities sites are expected to drop whatever they are doing and patch/take action immediately. Sites must act in 3 days. In this case EGI and WLCG management gives permission for services to be stopped/unavailable if necessary.

5.2.2 High Risk

- Most Root or admin exploits where the vulnerability has not been made public, where no public exploit exists, and only an authorised user can exploit the problem.
- Cases of identity theft and impersonation, where the exploit is not public
- Most cases in which an authorised user in principle can carry out destruction of data belonging to another group, but is not trivial
- Potential data leak which is illegal or embarrassing
- Denial of service which may affect a significant number of resources.

5.2.3 Moderate Risk

- Potentially serious, but hard to exploit problems, where no actual exploit has been written and producing one is seen as difficult. This may include hard to exploit buffer overflows, hard to exploit Race conditions
- Problem where a user can cause disruption to services but are easily traceable.

5.2.4 Low Risk

- Potential Denial of service at single site
- Vulnerability in actual software - but if configured as instructed not exploitable
- Potential vulnerability identified, but not clear how to exploit it

5.3 Vulnerabilities assessed as Critical risk

It is usually apparent quite quickly if an issue falls into one of the higher risk categories, and investigation tends to happen quickly. 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.

Here are some additional steps or considerations which may be considered if a vulnerability is assessed as 'critical' particularly if a fix is not available, for example in the case of a zero-day vulnerability. None are essential, and they may be done in any order.

5.3.1 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.

5.3.2 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.

5.3.3 Consider having an on-line conference to discuss the issue

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.

5.3.4 Actions recommended by SVG should be agreed before being carried out

It is not usually necessary to act in a matter of minutes. Any action taken, for example informing sites, asking them to act should ideally be agreed by several 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, without consulting SVG, but this is not an SVG action.

5.3.5 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.

5.3.6 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.

5.3.7 Decide whether to wait for a patch

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

5.4 Advisories and other notifications

The most common action is to issue an advisory 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.

5.4.1 Types of e-mail sent

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

HEADS UP – usually to warn sites or others if they are likely to be asked to do something urgently soon

Usually only sent for vulnerabilities assessed as 'Critical'

ADVISORY – Sites or others instructed to do something

The commonest type of mail, e.g., to update when vulnerability fixed in software or sites are asked to take other mitigating action.

ALERT – Should be aware

This may be important to you, you may want to act

INFORMATION – to inform of something

If a well talked about vulnerability is not relevant

Anything else we want to inform sites or others about

5.4.2 Traffic Light Protocol

For 'High' and 'Critical' vulnerabilities which are NOT already publicly disclosed the advisory is normally sent as TLP:AMBER . Mostly ALL advisories for HIGH and CRITICAL risk vulnerabilities are sent as TLP:AMBER to ensure that sites can take action before publicising that the EGI infrastructure may be vulnerable to a particular vulnerability.

Then made public at least 4 weeks after the vulnerability has been resolved to allow software to be updated or other action to be taken prior to making information public and placing on the public wiki.

For other issues it is sent usually sent as TLP:WHITE, and placed straight on the public web page

Other TLP values may be sent on discretion of the EGI SVG RAT.

5.4.3 Moderate and Low risk vulnerabilities

For issues which are announced publicly, where the software is not produced by those with which we collaborate, and is not in the EGI UMD or CMD, no action is usually taken.

Sometimes if a vulnerability is considered 'Low' risk, but people are asking about it or it is being talked about in the press, we may consider sending an 'informational'

For 'Moderate' and 'Low' risk vulnerabilities, where the problem is not announced elsewhere, and e.g. the software is developed by those with whom we collaborate, and/or is in the UMD we will send an advisory. In this case advisories may be typically short, and simply to inform people of the existence of the vulnerability, referring to the software provider.

5.4.4 Where to send

In most cases, it will be sites who are asked to do things.

Most advisories will go to

site-security-contacts@mailman.egi.eu - a list built from the CSIRT e-mail for each site in the GOCDB

ngi-security-contacts@mailman.egi.eu - a list built form the NGI security contact e-mail in in the GOCDB

noc-managers@mailman.egi.eu – ngi operation centre manager's mailing list

svg-rat@mailman.egi.eu – the RAT mailing list

csirt@mailman.egi.eu – egi csirt mailing list.

Note that the site-security-contacts@mailman.egi.eu - 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. Normally send when for most people, in Europe at least, it is office hours.

For vulnerabilities which only concern EGI Federated Cloud sites, mail may be sent to Cloud-sites-security-contacts@mailman.egi.eu instead of site-security-contacts@mailman.egi.eu

In some cases, an advisory may be sent to others, such as Virtual Organisations Security Contacts, if appropriate. Informing Virtual Organisations is at present carried out using the Broadcast tool in the OPS portal.

6 NDA for joining both the RAT the DEG

By joining the SVG RAT and/or the Deployment Expert Group you agree NOT to disclose any information you learn through your SVG participation about:

- how services or individual sites are deployed or configured;
- any specific software or configuration vulnerability;

except through official procedures of the EGI Software Vulnerability Group or with the agreement of the EGI Software Vulnerability Group

A simple e-mail reply saying ‘I agree’ is all that is required

7 References

No	*Description/Link*
R 1	EGI Strategy and Vulnerability Issue Handling Procedure https://documents.egi.eu/secure/ShowDocument?docid=3145
R 2	The EGI repository https://repository.egi.eu/
R 3	EGI services https://www.egi.eu/services/
R 4	EOSC hub portfolio https://confluence.egi.eu/display/EOSC/The+Hub+portfolio
R 5	EOSC marketplace https://marketplace.eosc-portal.eu/services
R 6	Best practices for handling software vulnerabilities – WISE working group https://wise-community.org/activities/