SOFTWARE VULNERABILITY GROUP (SVG) – TERMS OF REFERENCE

Document identifier	**EGI-SVG-TOR-108-V1**
Document Link	https://documents.egi.eu/document/108
Last Modified	**24/12/2010**
Version	**1**
Policy Group Acronym	**SVG**
Policy Group Name	**Software Vulnerability Group**
Contact Person	**Linda Cornwall (STFC)**
Document Status	**FINAL**
Approved by	**EGI.eu Executive Board**
Approved Date	**03/01/2011**

Purpose of this Document

The purpose of this document is to set out the Terms of Reference, composition and operating arrangements of the EGI.eu Software Vulnerability Group (SVG) and its Risk Assessment Team (RAT).

In EGEE-II and EGEE-III a similar activity was carried out by the Grid Security Vulnerability Group (GSVG). In the EGI proposal the need for a Software Vulnerability Group (SVG) was identified which carries out a similar function to the EGEE GSVG, but with a different scope.



I. COPYRIGHT NOTICE

II. DOCUMENT LOG

Version	Approval Date	Approved By	Amendment
1	03/01/2011	EGI.eu Executive Board	Initial version

TABLE OF CONTENTS

1 TITLE

The name of the group is Software Vulnerability Group ("SVG", hereafter also referred to as "the Group").

2 DEFINITIONS

Word/Term	Definition
CSIRT	Computer Security Incident Response Task Force
GSVG	The EGEE Grid Security Vulnerability Group
NGI	National Grid Initiatives
RAT	Risk Assessment Team
SVG	Software Vulnerability Group
UMD	Unified Middleware Distribution
OMB	Operations Management Board
EGI-InSPIRE PMB	EGI-InSPIRE Project Management Board

3 PURPOSE AND RESPONSIBILITIES

The Software Vulnerability Group has been established to reduce the number of software vulnerabilities in the EGI infrastructure.

The main purpose of the SVG is stated "to eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware, prevent the introduction of new ones and prevent security incidents" [R2].

The Risk Assessment Team (RAT) is established as the core working group within SVG and the main purpose is to handle specific software vulnerabilities reported in the EGI infrastructure. Most of the activities and responsibilities of SVG are done by RAT since software issue handling is by far the largest activity in the SVG. Having in mind sensitivity of software vulnerability issues some of the SVG responsibilities are only done within the RAT and cannot be performed by the SVG in general. These activities are:

- Providing a process for reporting, handling, and resolution of software vulnerabilities found in middleware made available to sites by the EGI Middleware Unit as the EGI Unified Middleware Distribution (UMD). This is the largest part of the activity, and the process is described in "The Vulnerability issue handling process", part of EGI-InSPIRE milestone MS405 [R2].
- Provide consultation on software vulnerabilities to the CSIRT Team and other EGI groups, including issues outside the scope of specific software vulnerability issue handling described above.

Vulnerability issues may by reported by e-mail to report-vulnerability@egi.eu. Vulnerability issues are written to a tracker to which the RAT has access. Only the RAT and those involved in the resolution of specific issues have access to information on vulnerabilities that have not been disclosed.

In the case vulnerabilities are announced publicly, SVG as the whole may discuss issues.

Furthermore, the SVG will be also responsible for:

- collaborating with others who assess software provided in the EGI UMD to look for vulnerabilities
- educating developers to encourage writing secure code, thus reducing the likelihood of the introduction of new vulnerabilities

Note that this group largely works on a voluntary/best efforts basis, and the amount of effort that can be put in depends on the good will of people, their institutes, and funding bodies.

4 AUTHORITY

- The Group is authorized by the EGI.eu Council through the EGI.eu Executive Board to investigate any activity within its Terms of Reference.
- The Group will comply with the Policy Development Process [R1]
- The EGI.eu Council and the EGI.eu Executive Board are the governing bodies of the Group.

5 COMPOSITION

5.1 Membership

Members of SVG include all RAT members. In addition, others may join provided they are members of a collaborating project or institute at the discretion of the chair, deputy, or RAT members.

Concerning RAT membership:

- Membership is drawn from the National Grid Initiatives (NGIs), sites, and organisations contributing software to the UMD.
- Members 'volunteer' their time and expertise to the group to further the aims of the Group.
- When members join the RAT they agree not to disclose confidential information concerning vulnerabilities to which they have access outside the confines of the group, without agreement from the group.
- No observers are allowed to the group since only those who are carrying out the issue handling can be members of the RAT

Concerning SVG membership not in RAT:

- Membership is drawn from the same places as the RAT, but additionally may be drawn from any organisation which has an interest in Grid Security Vulnerabilities
- Members 'volunteer' their time and expertise to the group to further the aims of the Group

The list of members is maintained on the SVG and RAT wiki (see Section 5.4.5 and 5.5.3)

5.2 Chair

The chair of the RAT and SVG is the same. The chair may nominate a deputy for both the RAT and SVG or just the RAT.

5.2.1 Duties

Concerning RAT activity, the duties of the Chair include:

- Ensuring that the issue handling infrastructure is in place, including the reporting mailing list, the tracker, web pages, and contact details with the various software providers for the UMD
- Ensure issues are handled in a timely manner, according to the defined process.
- Ensure all issues reported have an appropriate response and outcome, in a timely manner. If issues are beyond the scope this should be reported and some sort of appropriate action or not carried out.

- Report to management at regular intervals on the issue handling, including:
  - Number of new issues reported
  - Timeliness of initial issue handling
  - Number of open issues
  - Number of issues closed

Concerning the general SVG activity, the duties of the Chair include:

- Act as general point of contact for the Group
- Scheduling meetings and notifying group members
- Guiding the meeting according to the agenda and time available
- Ensuring all discussion items end with a decision, action or definite outcome
- Review and approve the draft minutes before distribution
- Liaise with others carrying out work on vulnerabilities, such as those carrying out vulnerability assessments and developer training
- Chair SVG sessions (including arranging speakers) in appropriate EGI Technical meetings/conferences
- Ensuring that the produced documents are presented for approval and adoption and that once approved these are published and made available in the document repository

5.2.2 Term of Office

The Term of the Office is unlimited.

5.2.3 Method of Appointment

The EGI.eu participant responsible for performing the duties of the SVG task appoints the Chair.

5.3 Secretary

5.3.1 Duties

Duties of the Secretary include:

- Assisting with the logistical details of meetings (be they face to face or phone/video)
- Support agenda preparation
- Taking and distributing minutes at the Group meetings
- Preparation and development of policy paper
- Assisting with the provision of, management and maintenance of document repositories and web(s) and wiki(s)

5.3.2 Term of Office

The Term of the Office is unlimited until the Chair appoints a new person.

5.3.3 Method of Appointment

The SVG Chair nominates the Secretary.

6 OPERATING PROCEDURES

6.1 Operating Procedures of RAT

We note here that if a vulnerability issue is reported, it is handled by those RAT members available. Any stakeholder of EGI also has the right to suggest new policies and procedures or revision of old policies and procedures which in their opinion need revision. These requests should be submitted to the Chair of SVG/RAT who will discuss with SVG/RAT during a subsequent meeting of the group. The decision whether to accept this request or not will be recorded in the minutes of the meeting and feedback will be provided to the original requestor.

6.1.1 Communications and Meetings – general

- Most of the RAT activity takes place by e-mail (all RAT members are subscribed by the chair to the mailing list), or by the report-vulnerability request tracker which is visible and modifiable by the SVG-RAT group (see Section 5.4.5).
- A quorum of members must be present before a meeting can proceed. At least 50% members must be present for the meeting to proceed.
- The Group will meet at least every three months – either face to face, by EVO or telecon.
- Where practicable, the agenda together with reports and documents that relate to the Group will be forwarded to members in sufficient time to enable consideration prior to meetings
- Accurate minutes will be kept of each meeting of the Group. The minutes of a meeting shall be submitted to group members for ratification at the next subsequent meeting of the Group

6.1.2 Communications and Meetings – specific vulnerability issues

- Note that if a vulnerability issue is reported, it should be handled usually over 2-3 days by those RAT members available at the time.
- Face to face meetings, and/or telecom or EVO meetings will be arranged if the RAT thinks it is helpful to discuss issues or problems.

6.1.3 Decision making – specific vulnerability handling process

- The process for carrying out vulnerability handling is described in the related material [R2].
- Any changes need to be agreed at least by the majority of the RAT members and approved by the EGI-InSPIRE PMB and OMB

6.1.4 Decision making – specific vulnerability issues

- When carrying out a Risk assessment of a reported issue, all RAT members will be invited by e-mail to give their opinion on the Risk Category.
- Except in the case of Critical issues, RAT members will be given at least 1 full working day to respond.
- At least 3 RAT members should give their opinion on the Risk category. Usually it will be more but as the aim is to investigate and assess issues within 3 working days we do not demand more than 3.
- Wherever possible, the Group will arrive at a proposed draft advisory or other recommendation documents and/or advice by clear consensus, as determined by the Chair
- A voting process on advisories and documents will only start if consensus cannot be reached in a reasonable time or if at least one third of voting members of the Group call for a vote

- A decision is adopted if more than 50% of the voting members cast their vote for the proposed decision
- If the Group's recommendations are adopted by majority vote, minority positions will be recorded and reported
- The Group may by majority decision refer matters for decision to the Director on issues where a consensus cannot be achieved.

6.1.5 Communication Channels

Communication channel	Reference
The Group mailing list	SVG-RAT@mailman.egi.eu
Main wiki page	https://wiki.egi.eu/wiki/SVG:RAT
Members	https://wiki.egi.eu/wiki/SVG:RAT_Members

6.1.6 Reports

- The Group produces advisories on vulnerability issues on a responsible disclosure basis and other recommendations which are agreed between the RAT and the software provider.

6.2 Operating Procedures of SVG

6.2.1 Communications and Meetings

- All the members of the Group are subscribed by the chair or deputy to the SVG mailing list and should use it as primary written communication channel. It is expected that most of the communication is carried out via this list (see Section 5.5.3).
- The EGI SVG will usually meet one a month by telecon or EVO to discuss any issues which are public or more general software vulnerability matters, such as vulnerability assessments carried out by collaborators or new types of vulnerability
- Where practicable, the agenda together with reports and documents that relate to the Group will be forwarded to members in sufficient time to enable consideration prior to meetings.
- A quorum of members must be present before a meeting can proceed. At least 40% members must be present for the meeting to proceed
- Accurate minutes will be kept of each meeting of the Group. The minutes of a meeting shall be submitted to group members for ratification at the next subsequent meeting of the Group.
- The Chair/Secretary should make sure that all the updates concerning the group's dates, agenda and minutes are posted on group's Wiki page.

6.2.2 Decision making

- Wherever possible, the Group will arrive at proposed draft recommendations documents and/or advice by clear consensus, as determined by the Chair
- A voting process will only start if consensus cannot be reached in a reasonable time or if at least one third of voting members of the Group call for a vote
- A decision is adopted if more than 50% of the voting members cast their vote for the proposed decision
- If the Group's recommendations are adopted by majority vote, minority positions will be recorded and reported

- The Group may by majority decision refer matters for decision to the Director on issues where a consensus cannot be achieved

6.2.3 Communication Channels

Communication channel	Reference
The Group mailing list	SVG-discuss@mailman.egi.eu
Web page on EGI.eu website	http://egi.eu/policy/internal/Security_Vulnerability_Group_SVG.html
Main wiki page	https://wiki.egi.eu/wiki/SVG
Members	https://wiki.egi.eu/wiki/SVG:Members
Meetings and minutes	https://wiki.egi.eu/wiki/SVG:Meetings
Documents	https://wiki.egi.eu/wiki/SVG:Documents

6.2.4 Reports

The group will report on general activities which have been carried out in the previous quarter.

7 EVALUATION

The SVG Group will produce an annual report to the Governing Body, in line with best practice that will be defined, which sets out how the Group has met its Terms of Reference during the preceding year.

The minutes of the groups will be formally recorded and available to the Governing Body.

8 RELATED MATERIAL

Name	Location
[R1] EGI.eu Policy Development Process	https://documents.egi.eu/document/169
[R2] The Vulnerability issue handling process	https://documents.egi.eu/document/47

9 AMENDMENT

These Terms of Reference can be amended by mutual agreement of the Group Members through consultation and consensus. The amendments must be approved by the Governing Body. The Group will review its Terms of Reference on an annual basis as a minimum.

The present Terms of Reference enters into force with immediate effect.

Dr. S. Newhouse
EGI.eu Director