SVG

The EGI Software Vulnerability Group (SVG)

The purpose of the **EGI Software Vulnerability Group (SVG)** is "*To minimise the risk to the EGI infrastructure arising from software vulnerabilities*".

This has been recently updated to say "*To minimise the risk to all service providers, infrastructures, users and other parties which interact with the EOSC-hub, arising from vulnerabilities in software deployed on the constituents of the distributed infrastructure. In essence, to minimise the risk of security incidents due to software vulnerabilities.*"

We provide some information on SVG Scope in the EOSC era.

The EGI SVG runs a procedure for handling software vulnerabilities reported which are relevant to the EGI infrastructure. This includes vulnerabilities announced by major providers, as well as software which is developed by collaborating projects and organisations used in the EGI infrastructure.

Advisories are issued by SVG as part of this process.

The EGI Operations Management Board (OMB) has formally approved the EGI Software Vulnerability Issue Handling Process.

However, this procedure is at present undergoing major revision. (Oct 2020)

- Terms of Reference (Note that these are currently undergoing revision.)

Intel and other processor speculative execution vulnerabilities (including Meltdown and Spectre)

Here SVG provides information that may be useful to various sites concerning the various SVG Speculative execution vulnerabilities

Software for use on the EGI infrastructure

SVG cannot dictate what software is in use on the infrastructure, especially in the rapidly changing environment.

If you are involved in selecting software for use in the EGI infrastructure, or developing software for use in the EGI infrastructure it is important that you take some of the responsibility for the security of that software.

To help, we have produced a Software Security Checklist of things that you should consider.

You may also be interested in joining the Deployment Expert Group. (DEG)

What if you find a software vulnerability?

If it has not been announced publicly:--

DO NOT discuss on a mailing list - especially one with an open subscription policy or public archive

DO NOT post information on a web page

DO NOT publicise in any way - e.g. to the media

IMMEDIATELY Report it to report-vulnerability (at) egi.eu

Vulnerabilities announced publicly may be reported to this address too, which may be serious either to EGI, EUDAT, or other services in the EOSC-hub catalogue. This ensure SVG is aware of them, and able to assess the impact.

See Reporters View

Main Tasks of the EGI Software Vulnerability Group

- Provide an efficient process to report, handle, and resolve software vulnerabilities in software used in the EGI infrastructure.

This is the largest activity of the EGI SVG.

- Provide consultation on software vulnerabilities to the CSIRT team and other EGI groups.
- Collaborate with other partners to identify vulnerabilities, and share information on vulnerabilities.
- Encourage developers to write secure code, thus reducing the likelihood of future problems, by education and awareness.
- Encourage all those involved in the selection and deployment of software to be aware of security, aware that software deployed should be under security maintenance and configured in a secure manner.

Incidents

If a vulnerability has been exploited, it is an incident, and is NOT handled by the EGI Software Vulnerability Group.

You should then follow the EGI CSIRT Incident Handling Procedure

- SEC01 EGI CSIRT Security Incident Handling Procedure

Also see the CSIRT Incident reporting

Several people are in both the EGI Incident Response Task Force as well as the Software Vulnerability group, so sending to either will probably get forwarded fairly quickly to the right people.

The Software Vulnerability Issue Handling process

The EGI Software Vulnerability issue handling summary contains a brief summary of the issue handling process, and links to further information.

- EGI Software Vulnerability Issue Handling Process

This has been updated and updates approved by the Operations Management Board in December 2015, further updated and updates approved by the OMB in November 2017.

This is undergoing revision at time of writing, to cope with the increased inhomogeneity of the infrastructure.

Other activities

Vulnerability Assessment is the proactive examination of software in order to find vulnerabilities that may exist. At present there is no funding to carry out this activity.

The SVG also encourages developers to write Secure Code Secure Coding

A poster is available summarising the work of SVG PosterSVG-2011.pdf (This is a little old, and rather focussed on Grid Middleware)