www.egi.eu
@EGI_eInfra

The EGI Software Vulnerability Group (SVG)

- what we do and how we are evolving

Linda Cornwall and the EGI SVG
RAL/STFC/UKRI

The work of the EGI Foundation
is partly funded by the European Commission under H2020 Framework Programme

Contents

- Purpose of the EGI Software Vulnerability Group (SVG)
- What we do
- SVG Issue handling procedure
- What changes are we seeing in our infrastructure
- Deployment Expert Group (DEG) and iRAT
- Scope
- Other plans
- Invite to be involved

Purpose of the EGI Software Vulnerability Group

To minimize the risk of security incidents due to software vulnerabilities.

What we do

- Main activity is handling software vulnerabilities reported
  - This is the majority of the work we do
- Been doing this since 2005, 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 handles vulnerabilities in software produced to enable services, which EGI endorses e.g. in UMD/CMD
  - SVG has been assessing the risk of vulnerabilities in other software according to how it is used in EGI
  - But NOT trying to substitute/compete with various other vulnerability activities external to EGI
  - Worked well when we had a relatively homogenous environment, especially the Grid
- We have also produced a Software Security Checklist https://wiki.egi.eu/wiki/SVG:Software_Security_Checklist
  - Criteria for selecting software to reduce the likelihood of software vulnerabilities

SVG Issue Handling Procedure

- Anyone may report an issue by e-mail to
  - report-vulnerability .at. egi.eu
- If it has not been announced as fixed by the provider, SVG contacts the software provider and the software provider investigates (with SVG member, reporter, others)
- If relevant to EGI the risk in the EGI environment is assessed, and put in 1 of 4 categories – ‘Critical’, ‘High’, ‘Moderate’ or ‘Low’
- If it has not been fixed, Target Date (TD) for resolution is set - ‘High’ 6 weeks, ‘Moderate’ 4 months, ‘Low’ 1 year
- Advisory issued by SVG
  - If the issue is ‘Critical’ or ‘High’ in the EGI infrastructure
  - When the vulnerability is fixed if EGI SVG is the main handler of vulnerabilities for this software, or software is in EGI Repository regardless of the risk.
  - If we think there is a good reason to issue an advisory to the sites.

Issue handling procedure -2

- Critical vulnerabilities are handled with top priority, aiming for an action within 1 day
  - Special Procedure
- Current Vulnerability handling procedure
  - https://documents.egi.eu/public/ShowDocument?docid=3145 (Approved in 2017)
- Most work carried out by EGI SVG Risk Assessment Team (RAT)

- So far this year
  - 33 Vulnerabilities reported
  - 15 advisories issued publicly - Including 8 assessed as ‘Critical’

What changes are we seeing

- Less vulnerabilities in software developed by people we know , less ‘in house’ software
  - Although there are still some
- Less vulnerabilities reported to us by those who discover them
- Some where developers tell us before telling the public
- Software vulnerabilities are ‘announced’ by the software provider
  - We are alerted to potentially relevant vulnerabilities which have been announced
- Less homogenous infrastructure
  - Greater proliferation of software
  - Current SVG members cannot be experts on all software used
  - Main motivation for change in the procedure

Deployment Expert Group (DEG) and iRAT

- Deployment Expert Group
  - Idea is to have a team of experts who are used to developing, selecting, and/or deploying software in their institute or VO
  - To provide wider expertise
- For a particular issue, DEG members with appropriate expertise volunteer to help assess a particular vulnerability => issue Risk Assessment Team iRAT members

Job of Deployment Expert Group Members

- Look out for and report vulnerabilities in software you are aware of being deployed in EGI
- Respond when asked if an issue is ‘In Scope’
- Volunteer for the iRAT if you have expertise on particular software after it has been defined as ‘In Scope’

Scope for detailed issue handling

- Software in the EGI UMD and EGI CMD
- Software deployed on the EGI infrastructure + EGI Services https://www.egi.eu/services/ (including EGI Checkin)
  - This includes relevant Linux OS distributions
  - This includes S/W we know is on the infrastructure - e.g. HTCondor, Singularity
  - This includes any software which is widely deployed - conditional of DEG participation.
- The 300 plus services in the EOSC catalogue - https://marketplace.eosc-portal.eu/services
  - NOT in scope for detailed issue handling at present

Other Plans

- Most of our info is on the EGI wiki, which has been deprecated, we will moved it to somewhere else and update it.
- Work on Vulnerability handling ‘best practice’ for EOSC and other services which are NOT in scope for detailed issue handling
  - This will be done in conjunction with WISE
  - We still want to help providers of services in the EOSC catalogue https://marketplace.eosc-portal.eu/services and others to minimize the risk of security incidents due to software vulnerabilities

Invitation to join the DEG

- Do you have expertise in software or software deployment?
- Would you like to join the Deployment Expert Group?
  - E-mail svg-rat .at. mailmain.egi.eu

EGI: Advanced Computing for Research

www.egi.eu
@EGI_eInfra

Thank you
for your attention.

Questions?

The work of the EGI Foundation
is partly funded by the European Commission under H2020 Framework Programme