Plans for the EGI Software Vulnerability Group

Linda Cornwall, STFC

HEPSYSMAN

2nd June 2015

Purpose of the SVG

"To minimize the risk to the EGI infrastructure arising from software vulnerabilities"

Changing situation

- Previous focus largely on Grid Middleware
  - SVG members had quite a lot of expertise on this
- Technology is changing
  - Especially the emergence of the EGI Federated Cloud
- A wider variety of software is being deployed
  - Cloud enabling software, software within VMs, VMs themselves
  - VO specific software
  - Other software deployed on sites
  - Some commercial, some which is produced by our collaborators
  - SVG members can't be expert in everything

Think Security

- SVG cannot dictate what software is deployed
  - Nor do we have the manpower to do an assessment on all software people want to deploy
  - So those developing or selecting software for deployment need to 'Think Security'
    - This includes any dependencies you are using
  - Consider
    - Is it good, well written, secure?
    - Is it under maintenance?
- Software which does something useful, and gets a job done is not necessarily secure
  - And if it turns out bad it might have to be turned off at short notice, and then it won't be so useful

Make sure software is not obviously bad

- Quick checks
  - Who wrote it?
  - Has anyone with security expertise looked/assessed it?
  - Is user input sanitized?
  - Does it e.g. contain any obviously bad constructs?
  - Does it comply with EGI data protection policy?
    - Note that this is being written
    - Software must comply with data protection legislation
  - Take a look through the code
- If you are a developer, read up on secure coding
  - I know there is more awareness now than there was a few years ago

Is the software under security support?

- How much it matters depends on the purpose
  - If the infrastructure depends on it it better be supported
  - If a large VO depends on it it also better be supported
- In what way is it 'under support'
  - Big company with lots of funds – **OK**
  - Funded support teams we know – **OK**
  - University or other institute which allows previous developers to work on problems in work time – OK ish
  - 'Hobby' or a previous developer might fix it one evening - **Hmm**
  - Unclear. Unsupported - **XXXX**
- And for how long is it under support?

Vulnerabilities found in software must be handled

- For software distributed by EGI (in the UMD) SVG is usually the main handler of vulnerabilities
  - Potential vulnerabilities are reported to us
  - We should have contact details for the developers
  - This is a must for TPs with which we have an SLA
- For commercial or other software – means of reporting vulnerabilities securely without creating public information should be available
  - If you select software, you should check that it has adequate vulnerability handling
  - and be alert to any vulnerabilities announced
  - and be ready to help SVG when necessary

If you find a vulnerability:

- IF it has not been announced publicly
  - DO NOT Discuss on a mailing list – especially one with an open subscription policy or which is archived publically
  - DO NOT Post information on a web page
  - DO NOT Publicise in any way without agreement of SVG
- DO report to SVG via

  report-vulnerability@egi.eu

  This creates a ticket in the report-vulnerability tracker, which will be seen by the SVG Risk Assessment team
  - Vulnerabilities announced publicly may be reported to this address too

Principles of EGI SVG vulnerability handling

- Issue handling carried out by the SVG Risk Assessment team (RAT)
  - RAT members have access to information on vulnerabilities reported
- Anyone may report an issue by e-mail to report-vulnerability@egi.eu
- If it has not been announced, SVG contacts the software provider and the software provider investigates (with SVG member, reporter, others)
- The relevance and effect in EGI are determined
- Then 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 for resolution is set - 'Critical' 3 days, 'High' 6 weeks, 'Moderate' 4 months, 'Low' 1 year
- Advisory is issued by SVG
  - When vulnerability is fixed if EGI SVG IS the main handler of vulnerabilities for this software, or software is in EGI UMD regardless of the risk.
  - If the issue is 'Critical' or 'High' in the EGI infrastructure

Note that there is no plan to change these principles

What HAS changed over the last couple of years

- SVG and CSIRT have worked more closely together
  - Incident Response Task Force (irtf) members who take an operational security duty also in the RAT
    - Can act if there is something serious/critical that can't wait
- For 'High' and 'Critical' issues if information is not public advisory sent to sites as 'AMBER'
  - Made public on wiki at least 2 weeks later
- Less manpower, sometimes having to process vulnerabilities with only 2 opinions on the risk
- Some not being fixed by Target Date

Work in progress

- SVG Terms of Reference rather out of date and needs revision
- SVG issue handling procedure is being updated
  - Plan to have new version in next couple of months, use for 6-12 months, then revise again if necessary
  - Using a number of recent vulnerabilities almost like ‘use cases’
- Plan to have all advisories in 1 place on the wiki
  - CSIRT alerts and SVG middleware advisories currently separate

Policy Violation

- For vulnerabilities which are Policy violations, Risk Assess but don't set TD
  - SPG and management handle
  - E.g. publicly readable DN vs usage of resources
  - A few of these recently – useful for logging purposes but doesn't comply with data protection legislation
  - We don't inform sites (yet)

Other points

- We have limited effort, if several vulnerabilities come at once then we will have to prioritize
- No guarantee that we won't miss something important
  - Hence the multi-pronged approach, vigilance from people deploying software as well as our procedure for handling vulnerabilities

Anyone interested in joining the RAT?

- We could do with more members – e.g.
  - For Risk Assessments
  - Experts in various pieces of software used in EGI
- Must be active, i.e. willing to do some work on vulnerability handling
  - Small % of your time
  - No 'observers'
  - It's a chance to influence the process

Summary of strategy for change

- SVG can't be an expert in everything, cannot guarantee to find every SW vulnerability that may be a serious problem
  - lots of vulnerabilities announced each year
- Everyone writing or selecting S/W for deployment should 'Think Security'
  - Whether VOs, CRPs, endorsing VMs, etc.
  - Then be clear who to contact within EGI/VO etc. in case of potential vulnerabilities
- Handle vulnerabilities according to the principles we have established over the last few years.

Point for discussion

- What if a vulnerability is not fixed on time?
- In the past, said we would release advisory on TD even if it isn't – Responsible Disclosure
  - Made sense when we were very separate from CSIRT
  - Also key to encouraging people to report to us
- In reality, often we don't as it doesn't help our sites
  - Now we are very close to CSIRT
  - 1 recently needed 6 months to fix a 'High'
    - Kept prompting and they kept apologising for delay
- Options
  - Tell sites? Tell management? Both?

Thank you for your attention.

Questions?