SVG status, summary, and plans

Linda Cornwall, STFC

EGI CSIRT F2F Abingdon 8th Sept 2016

www.egi.eu

Purpose of SVG

- "To minimize the risk to the EGI infrastructure arising from software vulnerabilities"
- AMBER removed version of slides

SVG issue handling - reminder

- 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
- 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

SVG issue handling – reminder -2

- Advisory is issued by SVG
  - When the vulnerability is fixed if EGI SVG is the main handler of vulnerabilities for this software, or software is in an EGI Repository regardless of the risk.
  - If the issue is 'Critical' or 'High' in the EGI infrastructure
  - If we think there is a good reason to issue an advisory to the sites.
- Advisory is 'Amber' if:--
  - 'High' or 'critical' risk and information is not public
  - There is some other reason to be Amber
  - Usually 'White' after 2 weeks assuming it is fixed
  - Otherwise usually white.

Vulnerabilities update – since April 2016

- 19 new vulnerabilities have been reported
  - 3 'Critical', 3 'High', 6 'Moderate'
- 15 advisories issued publicly
  - 2 Critical, 4 High, 4 Moderate, 5 low.
- At present 9 open tickets
  - 1 'critical' awaiting UMD release
  - Typically 8-15 open tickets at any one time, things do get resolved

AMBER

Functionality removed

- One issue concerned functionality on which we depend being removed by the software provider
  - Case "Authorization by user_id to manage VMs does not work in V2.1 Nova API for OpenStack"
  - This is a risk we missed in the risk assessment

Some other reminders

- All advisories are now in one place

https://wiki.egi.eu/wiki/SVG:Advisories

  - No more separate csirt alerts – all advisories/alerts in one place
- IRTF people are reminded they are in the RAT
  - Give an opinion on risk
  - Comment on the advisory and what is recommended
  - And unless 'Critical' we now give 2 days
  - IRTF has not handed over OS vulnerabilities to SVG, IRTF has joined SVG

Other To Do

- Notes on Risk – needs updating
  https://wiki.egi.eu/wiki/SVG:Notes_On_Risk
  - Including more on credentials needed to carry out the unintended action
- TOR - updated ages ago
  - can these be approved?
- Private wiki or other means of easy sharing non-public info
- Consider VO contacts for advisories concerning vulnerabilities, not just for cloud but other things

Fed Cloud related

- Fed Cloud people are responsive, when an issue relevant to Fed Cloud comes up
- Still 'Contact lists' needed
  - VM Endorsers
  - VM Operators
  - VM Creators ?
- Agreed it is a good idea to have VM Operator role
  - At present any member of a VO which is cloud enabled can instantiate VMs
    - Commonest usage at present
    - In future, envisage more users with less privilege

CMD

- There’s a plan to have all EGI cloud related tools in the ‘Cloud Middleware Distribution’ CMD
  - This is not available yet
  - But it means cloud tools will be handled in a similar way to Grid Middleware in the UMD
  - Don’t know when this will be available

Collaboration with other projects

- Need to work out the best way to collaborate/share information with other projects
  - Additional lists for 'Amber' and 'White' info?
  - Pre-warning some people, e.g. WLCG, OSG, EUDAT?
- Lightning talk (5 mins) at DI4R meeting called "prevention is better than cure"
  - Vulnerability handling one aspect to preventing incidents
  - Brief summary of what we do
  - Invite collaboration

Almost an aside - Risk Assessment

- Not much progress since April
- Plan to take the 25 top risks, try and get ‘Risk Owners’ to look at how to mitigate
- Noted 2 risks which probably need more consideration
  - Losing security functionality on which we depend
  - Ransomware – becoming a bigger issue
- Probable lightning talk at WISE meeting at DI4R concerning cloud risks

Thank you for your attention.

Questions?