www.egi.eu
@EGI_eInfra

The EGI Software Vulnerability Group (SVG)

Purpose, Why needed? And evolving for the future

David Crooks, Linda Cornwall and the SVG
RAL/STFC/UKRI

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

Purpose of the EGI Software Vulnerability Group

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

Some say we don’t need an SVG?

- Why not just trust that Services update, rather like our mobile ‘phones?
  - Much of the software e.g. linux may automatically update
- Why not just assume sites, services and facilities are competent and keep services patched?
  - Sites can easily look at advisories, make judgments for themselves
  - Sites are responsible for their own security
- Some say sites might not find our advisories useful

Reasons we need an SVG

- Want to be able to help data centres and services stay secure
  - Especially help smaller sites or sites without a lot of experienced staff
  - Give VOs and those using services confidence that their data is secure
- Sites and data centres are running software and implementing configurations which are non-standard
  - We need to be able to help them
- Sometimes e.g. RedHat advisory not correct in our environment, need to send out appropriate info
  - Risk may be higher or lower according to how software is used, how services operate
- SVG may advise sites to do something other than patch, some mitigating action if no patches are available

Reasons we need an SVG -2

- EGI CSIRT monitors for sites which are not patched and operations may suspend sites which fail to patch
  - Doesn’t seem reasonable to monitor and provide consequences if we don’t provide an advisory
- Some of the services depend on non-standard software to enable services, vulnerabilities in this software need to be handled
  - Although there is less of this than there used to be

What do we do now?

- Main activity is handling software vulnerabilities reported
- Largest focus has been on the Grid services
- Basically, we exist for the reasons we are needed

- And we have talked about what we do many times before

Going forward

How we do these things under discussion

- Looking to speed up our process - especially for vulnerabilities announced publicly
  - E.g. speed up assessment
  - Quicker/simpler advisories especially for vulnerabilities which don't need special investigation in our environment
- Looking to see if we can get sub-groups/other interested parties to deal with the wider variety of services and software
  - In particular to investigate the impact of vulnerabilities in different service types
- Improve our website

Invitation to be involved

- Are you interested in being involved in the Software Vulnerability Group?
- Do you have expertise in software or software deployment and would be interested in helping us keep the infrastructures secure?
  - This could be related to cloud, HTC, HPC, anything which you could help with relevant to EGI
- Would you like to be involved?
  - 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