Proposal for a new WISE working Group - Best Practices for handling Software Vulnerabilities

Linda Cornwall (STFC-RAL, UK Research and Innovation)

WISE virtual meeting, 29 Oct 2020

In collaboration with and co-supported by EU H2020 EOSC-HUB
Each of the collaborating infrastructures has the following:

[OS4] A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts.

[OS5] A process to manage vulnerabilities (including reporting and disclosure) in any software recommended for use within the infrastructure. This process must be sufficiently dynamic to respond to changing threat environments.

The idea of the new WISE working group is to give some best practice guidelines for these

And a little more including good practice for selecting software for deployment, what software providers (i.e. where our collaborators write software) do
EGI Software Vulnerability Group - basic procedure

• Anyone may report an issue by e-mail to
  • report-vulnerability@egi.eu
  • This may be a vulnerability discovered by the reporter, or it may be to alert SVG to a relevant vulnerability found/announced by a technology provider

• If appropriate 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

• ‘Critical’ - special procedure
Advisory issued by SVG

• Advisory is 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, and if software is in EGI Repository regardless of the risk.
  • If we think there is a good reason to issue an advisory to the sites.

• GOCDB lists all sites in infrastructure - including security contact
  • Info used to build e-mail list of sites we send advisories to.

• Sites are monitored for ‘Critical’ and ‘High’ risk vulnerabilities
  • Have a well developed monitoring system based on pakiti
  • Sites MUST patch ‘Critical’ risk vulnerabilities within 7 days or risk suspension

• We believe (but cannot prove!) that our issuing of advisories has prevented incidents
Changing infrastructures and technology

• Started mainly handling Grid enabling software, it was noted that some had security problems and no-one was addressing them
• Then moved to handling software vulnerabilities in all software enabling the distributed services
• Now there’s increasing proliferation of software, technologies, EGI is getting less homogenous
  • Those selecting software for deployment need to be aware of ensuring it is secure
  • Within EGI - encouraging more to participate in the handling of software vulnerabilities
• The EOSC-hub catalogue hosts 269 services https://marketplace.eosc-portal.eu/services
  • Need guidelines - so defining ‘best practice’ getting more important
Why a WISE working group on handling Software Vulnerabilities?

- WISE SCI is endorsed by many infrastructures so is a good place to carry out this work
- We can exchange information on what we do to avoid exposure to risk from vulnerabilities, what works and what doesn’t
- Provide guidance for infrastructures, sites and services on how to handle vulnerabilities to minimize exposure
  - 100s of services, would be good to have a short document defining best practice
- One service within an infrastructure may cause security problems for another
- Important that services advertised are as secure as possible, want to avoid reputational damage
- Possibly share workload concerning common problems
Possible areas we could consider

• Software providers guidelines - mainly for bespoke/collaborative software
  • What to do to minimize vulnerabilities and appropriately handle any found
• Infrastructure/service/site guidelines - main area
  • Selection of software
  • Handling of vulnerabilities
  • Patching
  • Monitoring
• Possible sharing of work/collaboration between sites/infrastructures/services
• Possibly sharing of intelligence on SW problems not yet public
Discussion

• Is it a good idea to have a new WISE working Group - Best Practices for handling Software Vulnerabilities?
• Is anyone interested in taking part?
• ?