Proposed WISE working Group – Best Practices for handling Software Vulnerabilities

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

WISE virtual meeting, 26th Oct 2021

SCI V2- Security for Collaborating Infrastructures Trust Framework

- https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf
- Operational Security - 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
- Possibly a little more including good practice for selecting software for deployment, and what software providers (in particular where our collaborators write software) do

Suggested Purpose of WISE WG on Software Vulnerabilities

"To define and share good practice in order to minimize the risk of security incidents due to software vulnerabilities in collaborating infrastructures"

Linda Cornwall

26 Oct 2021

Main areas for reducing software vulnerabilities

- Software development – good practice for those who write software, e.g. collaborative/in house software
- Software Selection, when selecting e.g. commercial software
- Handling vulnerabilities found/reported
- Monitoring sites for exposed vulnerabilities
  - Maybe this is part of handling software vulnerabilities?

Handling Software Vulnerabilities

- Procedure to report vulnerabilities relevant to the infrastructure, including
  - Inform software provider if appropriate
    - So they can fix them
  - Assess the risk to the infrastructure
  - Tell sites what to do for those considered serious, e.g. install patches, take mitigating action
- (EGI SVG and its predecessors have been doing this for around 15 years!)

Software selection – examples of what to consider

- Trusted well known (usually commercial) providers?
- Trusted people we collaborate with who write software used on or to enable the infrastructure?
- Other things to consider
  - Is software under security maintenance? How long will it remain so?
  - When was the last release?
  - Is there a procedure for reporting software vulnerabilities to the developers?
  - How are software vulnerabilities announced?

Why a WISE working group on handling Software Vulnerabilities?

- WISE SCI is endorsed by many infrastructures so WISE is a good place to carry out this work
- Provide guidance for infrastructures, sites and services on how to handle vulnerabilities to minimize exposure
- 100s of services in various places, including EOSC, would be good to have a short document defining best practice
- Important that services advertised are as secure as possible, want to avoid reputational damage

Start with Vulnerability handling

- Suggest start with document ‘Good practice for Software Vulnerability Handling’
- If we want to expand to other things we can later

What to call it - ideas

- SWVH – WG SoftWare Vulnerability Handling working group
- SWV – WG SoftWare Vulnerability working group. Then it could get expanded in future if we wish to avoiding getting them into software too.
- HSV-WG Handling Software Vulnerabilities working group
- VH –WG Vulnerability Handling working group.
- SVH –WG Software Vulnerability Handing working group - maybe
- BPSVH – WG maybe not

Discussion

- Is it a good idea to have a new WISE working Group – Best Practices for Software Vulnerability Handling?
- Do we want handling to include monitoring?
- Do we want to confine it to handling vulnerabilities, or to be broader and consider things like software selection?
- Is anyone interested in taking part?
- ?

??


WISE
COMMUNITY