WG-SVH
Software Vulnerability Handling Working Group

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

WISE virtual meeting, 21st April 2022

Defining best practice concerning the handling of software vulnerabilities

- Last October agreed it is a good idea to have a Software Vulnerability Handling working group
- Agreed the main aim is to define best practices concerning the handling of software vulnerabilities
  - Other things like secure coding, selecting software which is less likely to be problematic in terms of software vulnerabilities not done initially
- WG-SVH Software Vulnerability Handling WG

Description of WG-SVH

It is well known that exposed and exploitable software vulnerabilities may result in security incidents. The WISE SCI Trust Framework requires Infrastructures to have a process to manage vulnerabilities. This needs to be simple and usable, and as with any other form of security, it needs to balance security and availability according to the risk posed. The SVH WG will document agreed best practice concerning the handling of software vulnerabilities. This will include guidance for reporting newly identified vulnerabilities, as well as how sites and services should deploy the patching of software vulnerabilities after patches have been released. Central to this activity is the risk assessment of software vulnerabilities. Guidance on such risk assessment will be included in the document. How urgently a software fix is required, and how urgently services need to be patched depends on the risk. When the risk is sufficiently high this can justify the potential degradation or interruption of services in order to remove exposure to the vulnerability. This group will draw upon the experience of the group members, their Infrastructures and other best practice already available.

Linda Cornwall

Suggested 1 sentence Purpose of WG-SVH

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

Linda Cornwall

21 April 2022

EGI Software Vulnerability Group

- We have been handling vulnerabilities for around 15 years
  - Can draw on that experience

Why the need to document best practice?

- For many devices, updates are (semi) automatic
  - Mobile phones, standard laptops etc.
- For collaborating e-infrastructures, not that simple
- 3 main reasons why we need to document something
  - Need to handle software vulnerabilities in software which is written by those we collaborate with
  - Software is often used in non-standard ways
  - Ensuring that sites within an infrastructure are all aware of serious relevant software vulnerabilities and take action

Reporting/becoming aware of Vulnerabilities

- There needs to be a means of reporting vulnerabilities that are relevant to a given infrastructure
- This includes vulnerabilities ‘discovered’ by the reporter
  - Usually in software written by those we collaborate with
  - Rarely in e.g. commercial software
- Important that the reporting is not public, e.g. NOT in a public bug handling tool
- Consider that people should look out for relevant vulnerabilities in software they have expertise in
  - E.g. those who define how to setup services within an infrastructure

Then handling

- Some people need to carry out the handling of software vulnerabilities
- Inform software provider if appropriate
  - So that they can fix them
- Work out whether the vulnerability is ‘real’ and relevant/potentially exploitable in the infrastructure
- Assess the risk to the infrastructure
- Tell sites what to do for those considered serious, e.g., install patches, take mitigating action

Risk assessment

- Risk posed by a vulnerability needs to be assessed
  - This is key to deciding which vulnerabilities need to be acted on, and how urgently
- E.g. a vulnerability with a public easy to execute root exploit is far more serious than a possible local DoS.
- Publicly announced vulnerabilities may be less or more serious in distributed infrastructures, depending on how the software is used
  - Including because large numbers of people have access to a system/service
- Possibilities are CVSS score, ‘Critical’ ‘High’ ‘Moderate’ ‘Low’
- Also good to have consistency within an infrastructure or collection of services

Is the vulnerability fixed?

- If a vulnerability has not been fixed, may set a target date of fixing according to the risk
  - This is particularly the case for vulnerabilities in software written by those we collaborate with

Ask sites to take action

- How urgent, depends on risk
- This may be to patch/update if a fix is available
- This may be to carry out mitigating actions – especially if a vulnerability is ‘critical’ and no patch is available
  - Could even be to shut down services
- For more serious vulnerabilities, may set a timescale for sites to act
  - In EGI for vulnerabilities assessed as ‘Critical’ usually ask them to act in 7 days

Monitoring of sites for exposure to vulnerabilities

- In EGI sites are monitored for vulnerabilities which have been assessed as ‘High’ or ‘Critical’
- Ops team follows up on exposed ‘Critical’ vulnerabilities
- Up to national teams whether or not to follow up on ‘High’ risk vulnerabilities

Discussion/how to progress

- I suggest I start with a first draft
- Then distribute
- Then we meet and discuss
- Who is interested in collaborating on this?

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