EGI Software Vulnerability Group (SVG)

Linda Cornwall

EMI Security Workshop

25-26th May 2010 - CERN

Purpose of the EGI SVG

The main purpose of the Software Vulnerabilities Group (SVG) is “To eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware, prevent the introduction of new ones and prevent security incidents”.

3 main activities for reducing vulnerabilities

- Handling vulnerabilities found/reported
  - This was the largest activity of the EGEE Grid Security Vulnerability Group (GSVG)
- Assessing software for vulnerabilities
  - Resolving any found
  - Some done is SVG, some other groups
- Preventing new vulnerabilities being introduced
  - Developer education, awareness

Scope of SVG

- The main scope is to deal with software vulnerabilities in the EGI UMD software distribution
  - GSVG was very focused on gLite, SVG should cover all EGI UMD software distribution
  - Plus effects of vulnerabilities in dependencies
- SVG will also look at any Software Vulnerability problems that effect EGI on case by case basis

Issue handling process

- Similar to EGEE GSVG
  - But with increased scope to cover all software distributed by the EGI UMD (including EMI software)
- Anyone may report an issue
  - By e-mail to

  report-vulnerability@mailman.egi.eu
- Issue is investigated by a collaboration between the Risk Assessment Team (RAT), reporter and developers.

Issue handling (2)

- If the Issue is Valid, the RAT places in 1 of 4 risk categories

  Extremely Critical, High, Moderate or Low

- Target Date for resolution set according to the Risk

  EC - 2 days, High - 3 weeks, Moderate – 3 months, Low - 6 months

  This allows the prioritization of timely resolution

- It is then up to the developers and release team to get a patch out by the TD

  SVG will provide help an advice if appropriate

Issue handling (3)

- Advisory issued when patch is available or on Target Date – whichever the sooner
  - Advisory refers to release notes, release notes refer to advisory
- More details of EGEE GSVG process at http://www.gridpp.ac.uk/gsvg/
- Details will be revised (e.g. Target Date for the 4 risk categories) by those participating in the SVG

Software providers agree(d) to SVG process

- Service Level Agreement between Software providers and EGI mean that it is accepted that there will be an issue handling process
  - Agree to provide contact details, response time
- Providers are invited to participate in this
  - By participating influence the process

Call for participation!

- Increased scope means increased effort/experience needed
- Particularly need to expand the group to include more software security people beyond gLite
  - E.g. Unicore, ARC, ...
  - More gLite people still welcome!
- By participating, and providing manpower you will get to influence the process
  - As well as ensuring software provided by EGI is secure!

What is needed?

- RAT members
  - For investigation and risk assessment of reported vulnerabilities
  - Typically 10% or less
- Deputies
  - Some other people to run process, draft advisories, so someone is available on most working days
- Educators
  - To help educate developers in secure programming

Vulnerability Assessment

- This is about assessing existing Middleware for vulnerabilities
- First Principles vulnerability assessment by Elisa Heymann et al from Universitat Autònoma de Barcelona
- Other interested people (including as a 'hobby') assess software and point out problems
  - We need to consider whether this can be co-ordinated
  - reward? respect/non-monetary prize?