The EGI Software Vulnerability Group
Software Vulnerability Handling in EGI

Linda Cornwall, RAL/STFC

Contents

- What is a software vulnerability?
- Purpose of SVG
- How we handle vulnerabilities
- Something on our experience
- Evolving software vulnerability handling to changing technology

What is a software vulnerability?

- A weakness allowing a principal (e.g. a user) to gain access to or influence a system beyond the intended rights
  - Unauthorized user can gain access
  - Authorized user can
    - gain unintended privileges – e.g. root or admin
    - damage a system
    - gain unintended access to data or information
    - delete or change another user's data
    - impersonate another user

Purpose of SVG (in EGI InSPIRE)

"To eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware, prevent the introduction of new ones and prevent security incidents"

Activities to reduce software vulnerabilities in EGI infrastructure

- Handling vulnerabilities found/reported
  - Main activity of SVG
- Assessing software for vulnerabilities
  - Formally and informally
- Preventing new vulnerabilities being introduced
  - Developer education, awareness
  - Considering new software to be used in the infrastructure

Grid Middleware vs other software

- The issue handling is largely designed to handle vulnerabilities in Grid Middleware
  - Where vulnerabilities are found in the software by the reporter
  - And EGI has a close relationship with the software providers
  - EGI SVG is main handler of vulnerabilities in this S/W
- Other software vulnerabilities are also handled – if the software is deployed in the EGI
  - Typically provider announces fix (e.g. Linux)
  - But occasionally a vulnerability ‘discovered’ by reporter reported to us

Issue Handling process

- This is carried out by the SVG Risk Assessment Team (RAT)
  - RAT members include middleware experts, security software experts, and EGI Incident Response Task Force (IRTF) members
  - The RAT has access to information on vulnerabilities reported
- Anyone may report an issue
  - By e-mail to report-vulnerability@egi.eu

Investigation of Vulnerability

- If issue is ‘discovered’ by the reporter, it is investigated by a collaboration between the RAT, reporter and developers
- Alternatively, if it is announced, it’s relevance to EGI and affect on is considered

Risk Assessment

- If the Issue is valid or relevant to EGI, the RAT carries out a risk assessment
- Issue placed in one of 4 risk categories

  Critical, High, Moderate or Low
- Risk assessment carried out by the RAT because
  - mitigating or aggravating factors may exist in the Grid environment
  - Usually by consensus – vote in principle but usually agree the risk category

Target date for resolution

- If developers need to produce a fix, Target Date for resolution set according to the Risk
  - Critical - 3 days, High - 6 weeks, Moderate – 4 months, Low - 1 year
  - Aim to reach this point within 4 working days
    - Within 1 day for critical issues
  - This allows the prioritization of the timely resolution of issues according to their severity

Fixing problem

- It is then up to the developers and release team to try and fix the problem by the Target Date or earlier
  - SVG will provide help and advice if appropriate
  - Advisory issued when patch is available or on Target Date – whichever the sooner
    - Advisory refers to release notes, release notes refer to advisory
  - This is known as responsible disclosure
  - EGI doesn't issue advisories vulnerabilities announced by the provider unless it's Critical or High.

When fix is available

- CSIRT monitors ‘Critical’ and ‘High’ risk vulnerabilities in the Grid Infrastructure
- For ‘Critical’ vulnerabilities, sites MUST update within 7 days
  - CSIRT issues tickets for sites which are vulnerable
  - Non-response may lead to site suspension

Result of experience

- A lot of vulnerabilities due to basic errors
  - File permissions
  - Not sanitizing input
- New vulnerabilities appear in well established software
  - E.g. when new functionality is added
- Vulnerabilities in software which is not well supported have been problematic

Contact and maintenance

- For Grid Middleware (EMI/IGE) SLA between EGI and project, vulnerability handling by EGI SVG – OK, fine
- For Linux (e.g. RedHat), carry out their own handling, and EGI just has to decide risk in our environment. – OK, fine
- For some software deployed, difficult to get response/fix from company when security problems found **NOT OK**

Evolving EGI SVG

- EGI SVG will need to replace ‘Grid Middleware’ with ‘Middleware associated with the sharing of Distributed Resources’
- At present, this means including the EGI federated cloud
- Possibly more commercial software, and other software where we don’t (yet) have a direct relationship with providers
  - Providers announce a vulnerability when it is fixed
  - We will be considering the Risk to our infrastructure rather than investigating the vulnerability and arranging for the developers to fix it

Expanding the ‘RAT’

- To handle vulnerabilities found relevant to the EGI federated cloud the RAT will need to expand to include:
  - Cloud Technology experts
  - Cloud Federation developers
  - Cloud security people

Important message 1 – if you find a vulnerability

- DO NOT
  - Discuss on a mailing list – especially one with an open subscription policy or which is archived publically
  - Post information on a web page
  - Publicise in any way without agreement of SVG
- DO report to SVG via

  report-vulnerability@egi.eu

Important message 2 – Software needs to be under security support

- If the software you use is NOT under security support – it's difficult to get vulnerabilities fixed if any are found
- We may have to say it cannot be used on the EGI infrastructure if it provides a security threat
- You can't assume even well established software won't have vulnerabilities

Important Message 3 – cloud people needed in the RAT

- If you are a cloud technology expert, cloud programmer, cloud security person, and think you could contribute to vulnerability handling consider volunteering for the RAT

Questions?

- ??