Software Vulnerability Issue handling after the end of EMI and IGE

Dr Linda Cornwall, STFC/RAL.

EGI Community Forum 2013

Contents

- Context
- General Procedure – reminder
- What is changing

Purpose of SVG

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

This continues to be the purpose of SVG

Main scope of SVG

- The main scope is to deal with software vulnerabilities in the EGI Unified Middleware Distribution (UMD)
- Also handles other software (jointly with CSIRT) to provide consistent risk assessments
- This does not change

What do you do 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

  This does not change

Issue Handling process

- This is carried out by the SVG Risk Assessment Team (RAT)
  - The RAT has access to information on vulnerabilities reported
- Anyone may report an issue
  - By e-mail to report-vulnerability@egi.eu
- Issue is investigated by a collaboration between the RAT, reporter and developers.

Issue Handling (2)

- If the Issue is valid, 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 - the RAT usually agrees on the category
  - Say vote, but mostly agree on category

Issue Handling (3)

- 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

Issue Handling (4)

- 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

Critical Vulnerabilities

- A special process is carried out
- This includes alerting all concerned (CSIRT, EGI Middleware unit, developers)
  - Consider whether it is possible to produce a patch in a short timescale
  - Whether a longer TD should be set –
    - It might be agreed that a patch can be produced in 1 week and CSIRT can live with it for 1 week
  - Whether mitigating operational action should be carried out – CSIRT advise on

In Principle

- Nothing is changing
  - General Procedure remains the same
- Some details of the procedure have changed
  - E.g. for ‘High’ risk issues advisory only to sites initially and make public 2 weeks later
- Details of how we contact people/how the procedure is carried out is changing
- Details not fully defined yet

Minimum needed for SVG to continue

- Direct contact details for product teams
  - Developers plus ‘responsible’
- Product teams respond a.s.a.p. and participate in investigation
- Product teams and UMD people produce patch in time for Target Date
- RAT continues
- Co-ordination continues

EMI 3

- EMI 3 will be supported by development teams for 1 year
  - Mostly the same individuals will be supporting the software
  - Including fixing vulnerabilities
- Products will be in the UMD
- The TD will continue to be the date by which vulnerabilities should be fixed in the UMD

EMI => MeDIA

- Middleware Development and Innovation Alliance (MeDIA) is being formed
- This will co-ordinate the development and support of Middleware enabling the sharing of distributed resources
- Discussion between EGI UMD and EMI this week
- MeDIA first meeting on 22nd April
  - After this things may be clearer

IGE => EGCF

- Globus in Europe will be coordinated by the European Globus Community Forum (EGCF)
- Details for how we contact appropriate people still require some clarification

Reminders

- SVG does not fix problems
  - But some members may happen to be in product teams
- SVG does not normally test fixes
  - Have to trust the product teams they really have fixed vulnerabilities
  - Less work likely to be carried out after end EMI and IGE

Proliferation of software

- Proliferation of middleware will probably mean that Product Teams will need to be more active in investigation
  - RAT members can't know everything
- Multitude of platforms and versions means we need better version tracking
  - Need to ensure versions all fixed at once
  - Looking into using OVAL
  - Will discuss when further progress on how things work

Some concerns

- In EGI SLAs defined response times
  - Likely to not be SLAs with product teams
    - In past either same project or SLA
  - How reliable will response be?
  - Not just a problem for vulnerabilities, but any serious software problem

Changing Technology

- EGI SVG will need to replace ‘Grid Middleware’ with ‘Middleware associated with the sharing of Distributed Rescores’
- Whether this be Clouds, or whatever the future holds
- A lot for SVG to think about

Questions?

??