Software Vulnerability Group (SVG) Update on issue handling

Dr Linda Cornwall, STFC/RAL.

EGI Technical Forum 2013

Contents

- General Procedure – reminder
- Update post EMI and IGE
- Numbers from the last year
- General experiences
- What’s 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”

Main scope of SVG

- The main scope is to deal with software vulnerabilities in the EGI Unified Middleware Distribution (UMD)
- Also handles other software widely deployed in the EGI infrastructure
  - Linux (jointly with CSIRT)
  - Other 3rd party.

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

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 – vote in principle but usually agree the risk 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

Since end of EMI

- General Procedure remains the same
- Former EMI software
  - Middleware Development and Innovation Alliance (MeDIA)
  - Post EMI technology providers list is being maintained
  - Product teams are actively fixing vulnerabilities

Globus software

- Globus software post IGE
  - European Globus Community forum (EGCF)
  - Security e-mail contacts provided for informing globus and EGCF of vulnerabilities
  - 1 vulnerability fixed in globus since end IGE.

Minimum needed for SVG to continue – as stated at UF

- 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

So far this is happening

Numbers from last year

- 36 Vulnerabilities reported
  - 24 in last 6 months
- Risk categories – 2 ‘critical’, 7 ‘high’, 8 ‘moderate’, 6 ‘low’
  - Some not assessed (not relevant/out of scope, invalid, duplicate, problems with single instances quickly fixed, no action needed)
- Majority (26) concern Grid Middleware

General experience

- A lot of vulnerabilities still due to basic errors
  - File permissions
  - Not sanitizing input
- As far as we are aware, no incidents due to Middleware vulnerabilities
  - Maybe we are just not interesting enough
  - Better to be a bit paranoid than have a load of incidents
- Vulnerabilities in non-Linux, non-Grid widely deployed s/w hardest to get resolved

Proliferation of software

- Proliferation of software in use in EGI 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
  - This was put aside over summer, until post EMI/IGE settled down

VOs greater role in security

- Identified by CSIRT and SVG that VOs are getting a greater role in security
  - Operate Workload Management systems, Instantiate Virtual Machines
  - Incident associated with specific VO
  - Vulnerability primarily affecting users
- Need VO security contact information
  - Both per VO and VO-security Contacts list
  - Brief requirements document produced

Changing Technology

- EGI SVG will need to replace ‘Grid Middleware’ with ‘Middleware associated with the sharing of Distributed Resources’ in the longer term
- Whether this be Clouds, or whatever the future holds
- Possibly more commercial software, and other software where we don’t (yet) have a direct relationship with providers

Questions?

??