Grid Security Vulnerability Handling and Risk Management

Linda Cornwall

EGEE'08 Conference, 22-26th September 2008, Istanbul, Turkey

www.eu-egee.org

e-infrastructure

Contents

- Summarize the EGEE strategy for handling and preventing Grid Security Vulnerabilities
- Provide a status update
- Describe plans for a General Security Risk Assessment to be led by the Security Co-ordination Group (SCG)

Hopefully leading to increased trust and confidence in the security of the deployed infrastructure from all parties

The Grid Security Vulnerability Group (GSVG)

- Started in EGEE-II, continuing in EGEE-III
- "The Purpose of the Grid Security Vulnerability Group is to eliminate Grid Security Vulnerabilities from the software, and prevent new ones being introduced. The aim is to provide a high level of confidence in the security of the deployed infrastructure, thus reducing the risk of incidents."
- Largest part of the work is the handling of specific Grid Security Vulnerability issues as they are found

People involved in GSVG issue handling

Linda Cornwall, Stephen Burke (RAL, UK)

Vincenzo Ciaschini (INFN, Italy)

Ákos Frohner, Maarten Litmaath, Romain Wartel (CERN)

Oscar Koeroo (NIKHEF, Holland)

Daniel Kouril (CESNET, Czech Republic)

Kálmán Kővári (KFKI-RMKI, Hungary)

Eygene Ryabinkin (RRC-KI, Russia)

Åke Sandgren (HPC2N, Sweden)

John Walsh (TCD, Ireland)

GSVG Issue handling summary

- **This was established and approved in EGEE-II**
- **Anyone may report an issue**
  - By e-mailing to grid-vulnerability-report@cern.ch or
  - By entering in the GSVG savannah https://savannah.cern.ch/projects/grid-vul/
    - Note that bugs are private so cannot be read except by members of this savannah project
- **The Risk Assessment Team (RAT) investigates the issue, if valid carries out a Risk Assessment**

Risk Assessments

- **RAT investigates the problem and discusses the risk**
- **Each valid issue is placed in 1 of 4 risk categories**
  - Extremely Critical
  - High
  - Moderate
  - Low
- **Target Date for resolution set according to risk**
  - EC – 2 days
  - High – 3 weeks
  - Moderate – 3 months
  - Low – 6 months.
- **This allows for the prioritization and timely resolution of vulnerabilities**

Disclosure

- **Information kept private – until advisory is released**
- **Advisory released on**
  - Target Date or
  - When a patch is issued
    - Advisory refers to the release
    - Release notes refer to the advisory
  - Whichever is the sooner
- **Advisories are released on the GSVG web page at http://www.gridpp.ac.uk/gsvg/advisories/**

  (earlier advisories were in the release notes)

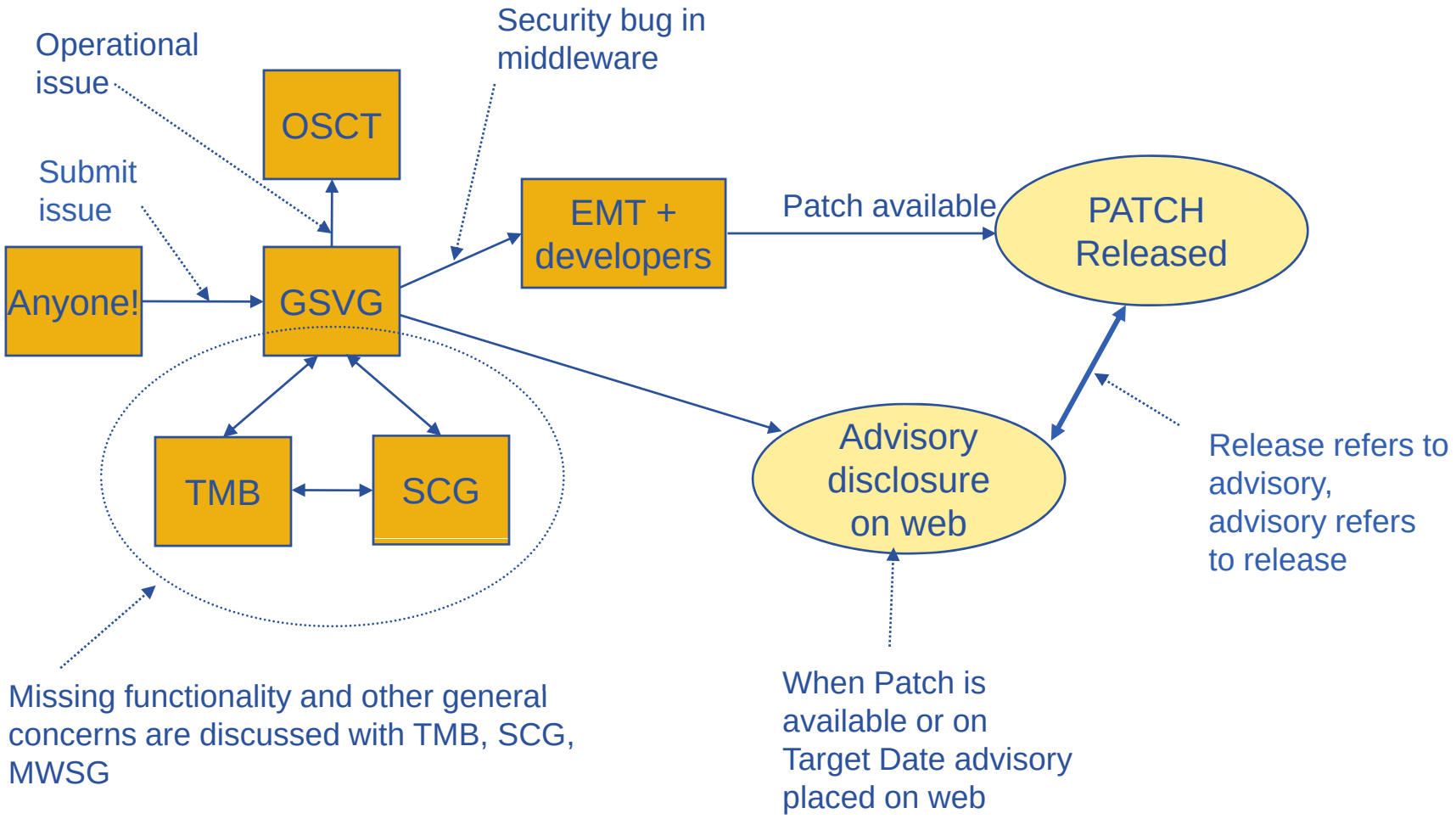
Why this strategy?

- Information is kept private except for those who are involved in the resolution of an issue to reduce the risk of exploitation
- Providing a Target Date allows the prioritization of resolution
- Information is disclosed in a timely manner to provide confidence in the system

Types of issue

- **Most issues result from Bugs in gLite Middleware**
  - Handled as described
- **Some result from bugs in 3rd party software**
  - Handled in a similar way
  - We don't release advisory on Target Date unless issue is fixed without permission from software provider, or the software provider has already made the information public
- **Operational issues**
  - Produce advisory to OSCT
  - Risk assessment not essential
- **General Concerns/missing functionality**
  - These are raised more broadly within project (SCG/TMB)

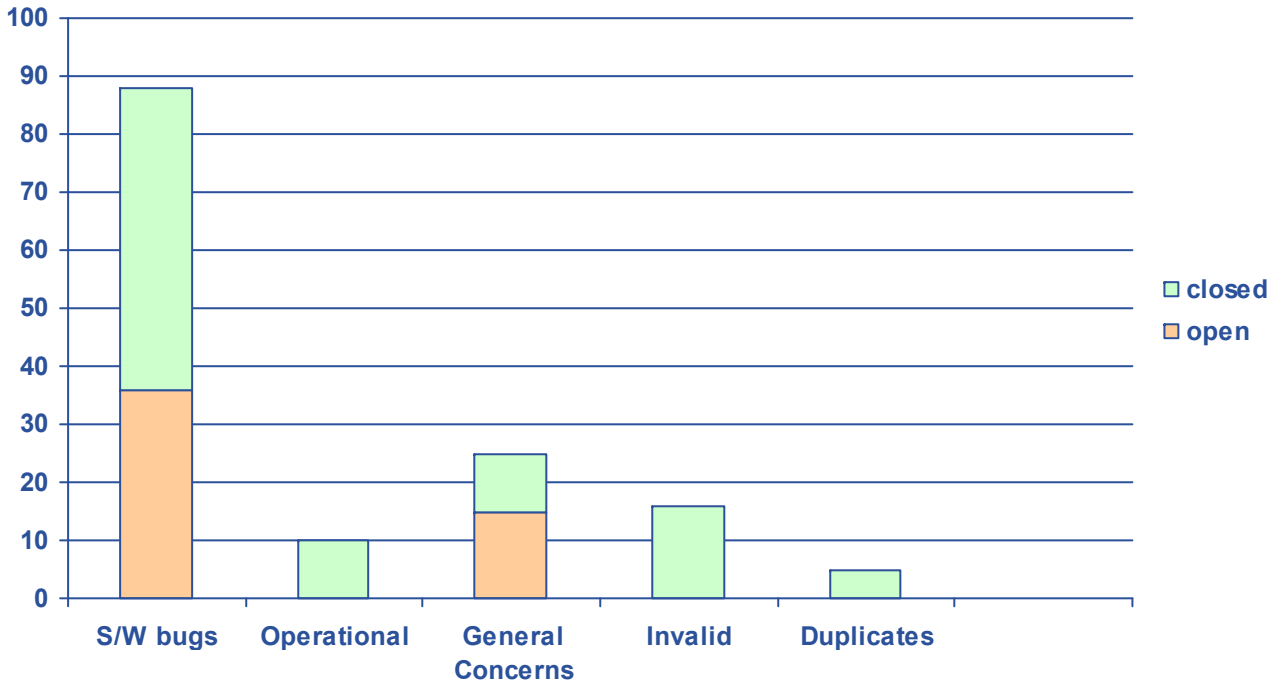
Basic interactions with other groups in EGEE-II



Some numbers (16th Sept 2008)

- **144 issues submitted since work began in 2005**
- **93 closed**
  - 49 fixed, 15 invalid, 5 duplicates, 5 software no longer in use, 10 general concerns, 9 OSCT informed
- **51 open**
  - 3 before TD, 15 general concerns/missing functionality, 14 disclosed (still open), 2 3rd party (OSCT knows about them), 8 other, 9 in work (but not disclosed)
- **Some of the more general concerns/missing functionality are the ones that seem to be open long term without resolution**
  - Need new approach

Current status – 16th Sept 2008



More on Advisories

- **Important not to disclose publicly ‘how to exploit’**
- **Should say ‘how to remove vulnerability from your deployment’**
  - Usually on public web page recommend installing patches
- **If a problem requires an operational solution, and details of how to fix reveals how to exploit – this should not be on a public web page!**
  - We send to the OSCT list
- **Plan to include ‘who may be affected’ or ‘who is at risk’**
  - E.g. VO, site, user…

Issues that are not straightforward bugs

- **Some issues result from missing functionality or more general concerns**
  - Cannot be simply handled by asking a developer to fix them
- **These are the main ones that seem to remain open long term**
- **Some require a change in the design, or new software to be developed**
- **Generally very well known within the project**
- **These have been documented in https://edms.cern.ch/document/950000/1**

Issues which are not bugs (2)

Some examples:

- **Middleware code integrity must be assured**
  - Strong desire for software signing
- **Outbound IP access should be restricted**
  - Outbound access needed for pilot jobs
  - Dynamic connectivity service was considered
- **No unique tracing of external actions from a WN**
  - Improvements to logging is being carried out

Code walkthroughs and testing

- In EGEE-II work was carried out at Poznan by the PNSC security team
- Various packages were reviewed (e.g. R-GMA, LFC)
- Result of reviews and testing revealed problems
  - Reports were written
- These treated as vulnerability issues
- If any future reviews take place, this strategy will continue

Vulnerability prevention

- We also want to prevent new vulnerabilities from being introduced
- A checklist was produced prior to EGEE-II, but this was not used – probably document too long
- Alongside EGEE-II, ISSEG project looked at education on security, including a checklist for developers

  http://isseg-training.web.cern.ch/ISSeG-training/
- Poznan has also produced a document on Security Best Practices for administrators, developers and users of the EGEE infrastructure https://edms.cern.ch/document/926685/1
  - This includes detailed instructions on how to avoid some types of vulnerability
- Plan to put information together on how to prevent vulnerabilities in 1 place– ensure developers guide refers to this

3 Common Types of vulnerability

- **File permissions**
  - E.g. world writable executable directory
  - One of the easiest to prevent yet a common cause of vulnerabilities
- **Input not sanitized**
  - mySQL injection vulnerabilities
  - XSS vulnerabilities
- **Buffer overflows**
  - Still get these
  - Careful with constructs

These are easy to prevent

The Security Assessment Plan

- **The Security Assessment Plan is an EGEE-III milestone https://edms.cern.ch/document/929864/1**
- **Describes the Plan for the on-going assessment of operational and Middleware security**
- **This includes 2 metrics for vulnerability handling**
  - 1 to measure the timeliness of GSVG handling
  - 1 to measure the timeliness of resolution of issues
  - Soon should formulate within GSVG and start using them
- **Also includes an Overall Security Risk Assessment**
  - Which will be led by SCG

Overall Security Risk Assessment

- **In LCG in 2003 a security Risk assessment was carried out**
  - 44 high level risks were described
    - E.g. misuse of resources to attack other systems, unauthorized distribution of data…
  - Committee decided on the risk value
  - http://proj-lcg-security.web.cern.ch/proj-lcg-security/RiskAnalysis/risk.html
- **Plan to re-visit these Risks, and any others that we consider appropriate**
  - But with a greater emphasis on what to do to reduce the Risks
- **SCG will lead this – with input from various members of the various security groups**

Overall Security Risk Assessment (2)

For each identified Risk the plan is to do the following

- Describe the risk
- Produce a numerical value for the risk
- Describe what is currently being done to reduce this risk
- Describe what should be done (if necessary) to reduce this risk

This will allow the prioritization of the mitigation of the most serious security risks

Also, re-visit at the end of the project to see to what extent risks have been reduced

Overall Security Risk Assessment (3)

- **Some of the Missing functionality/general concern type GSVG issues could be considered additional risks, or addressing them could reduce some of the overall risk**
  - These may form input to this process
  - Some may be additional risks
  - Some may need resolving to mitigate higher level risks
- **This General Security Risk Assessment will complement GSVG work on specific issues in the database**
- **Some GSVG issues/concerns may get moved to this more general risk assessment**

GSVG issue => Risk

- **Risk = Malicious middleware is distributed**
- **GSVG issue = Middleware code integrity must be assured**

  Compute Risk => If scores highly then good case for software signing

- **Risk = Resources used to launch attack on other sites**
- **GSVG issue = Outbound IP access should be restricted**
  - Compute Risk => If scores highly then good case for implementing software to e.g. restrict outbound access to other sites, log access, produce proposed dynamic connectivity service

Conclusions

- **The GSVG issue handling is operating well for issues that result from bugs in gLite middleware**
  - RAT members tend to agree on the risk
  - Process is well established and accepted
- **Passing information to OSCT is working well for operational issues**
- **Possibly we need to consider improvement to handling of VO software issues and 3rd party issues**
- **Issues arising from design problems, missing functionality or general concerns need some improvement – this may partly come from the more general Security Risk Assessments**

Further information

- **GSVG webpage http://www.gridpp.ac.uk/gsvg/**
  - Includes summary of issue handling process, advisories, links to documents
- **Security assessment plan https://edms.cern.ch/document/929864/1**

Questions/Discussion?

- ???