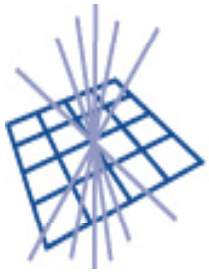


GridPP
UK Computing for Particle Physics

RAL 1957 2007
Celebrating 50 years of world class science

# The Grid Security Vulnerability Group

***Dr Linda Cornwall, Rutherford Appleton Laboratory ,***
***Harwell Science and Innovation Campus, Didcot, OX11 OQX United Kingdom***

*EGEE'07, Budapest, 3rd October 2007*

www.eu-egee.org

Information Society and Media

# Contents

- Stated aim of the GSVG in EGEE-II
- Setup and people involved
- GSVG process and Strategy
- Risk Assessments
- Some numbers
- What is going well
- What still needs improvement
- Issues that are not simple bugs
- Developers guidelines
- What we have learnt
- Any Questions?

# Stated aim in EGEE-II

- **The aim is "to incrementally make the Grid more secure and thus provide better availability and sustainability of the deployed infrastructure"**
  - This is recognition that it cannot be made perfect immediately
- **Main activity is to handle specific Grid Security Vulnerability issues which may be reported by anyone**

# Setup of the issue handling in EGEE II

**The GSVG issues group in EGEE II consists of**

- **Core Group Members**
  - Run the general process
  - Ensure information is passed on
  - 1 on duty each working day
- **Risk Assessment Team (RAT)**
  - Carry out Risk Assessments
  - At present 8 full RAT members
  - Plus 4 others which confine their work to their own area of expertise
- **RAT people are security experts, experienced system administrators, deployment experts and developers**

# People involved

Linda Cornwall, Stephen Burke, David Kelsey (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 )

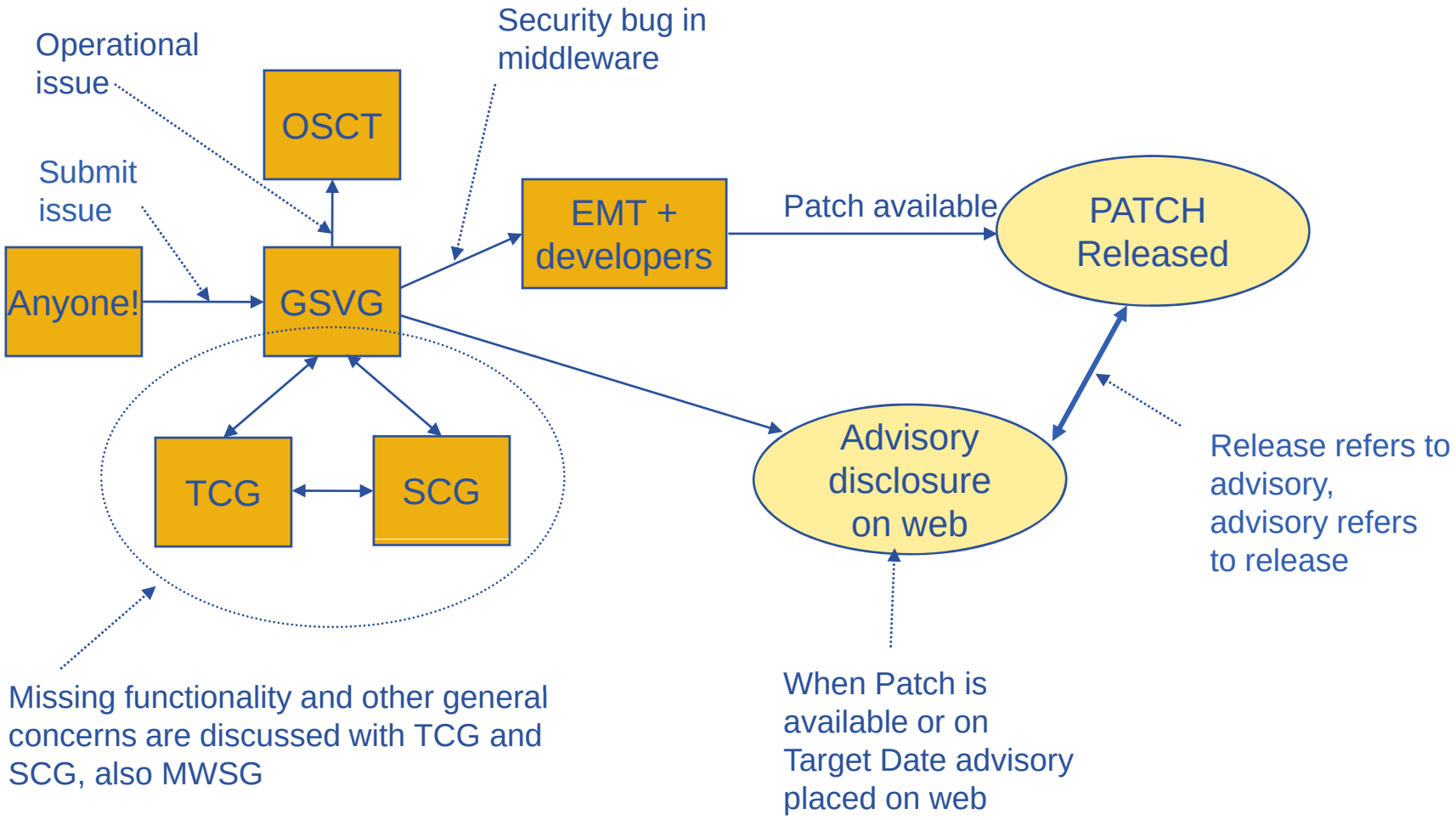
# Process and strategy in EGEE-II – to first order

- **Issue may be submitted by anyone**
  - e-mail grid-vulnerability-report@cern.ch
- **Risk Assessment carried out by the Risk Assessment Team (RAT)**
  - GSVG investigate issue
  - If issue is Valid, placed in one of 4 risk categories
  - Extremely Critical, High, Moderate or Low
- **Target Date for resolution set according to Risk**
  - Fixed – 2 days EC, 3 weeks High, 3 months Moderate, 6 months Low
- **Information kept private until advisory is released**
  - Only RAT and those involved in resolution are informed
  - (Unlike pre-EGEE-II)
- **Advisory released when issue fixed or on Target Date, whichever is the sooner**
  - (At least for EGEE/glite software)

# Types of issue

- **For Issues that involve a bug in the gLite middleware**
  - majority of issues are this type
  - Produce a special bug for JRA1 with a Risk and Target Date (TD) attached
  - Produce an advisory
  - Place the advisory on the web page when patch released or on the TD
  - In future we plan to send advisory to open subscription mailing list
    - Need to sign mails – otherwise it becomes a vulnerability!
- **For operational issues**
  - Produce an advisory to OSCT
  - OSCT inform sites as appropriate
- **Other types of issues/concerns**
  - Inform TCG/SCG/MWSG for discussions as appropriate

# Basic interactions with other groups in EGEE-II



# Risk Assessments

- **An agreed strategy where risk assessments are objective not subjective is required**
- **Site security officers most fear an attack that gives access to the whole site**
  - Especially if it can be carried out anonymously
  - DoS tends to be considered no more than medium risk
- **A vulnerability that can be exploited by an authorized user is considered by most less serious than one that can be exploited without credentials**
  - Especially if their actions are clearly logged
- **We can't ignore the possibility that credentials may be stolen**
- **Issues that can be exploited trivially and reliably are considered more serious than those that are harder to exploit and can only be exploited in rare circumstances**
- **Decided on 4 risk categories**
  - Extremely Critical
  - High
  - Moderate
  - Low

# 4 Risk Categories

- **Extremely Critical**
  - Examples
    - Remote Root access with or without Credentials
  - Target Date – 2 days

- **High**
  - Examples
    - Identity theft or impersonation
    - Exploit against MW component that gives elevated access
    - Grid-wide disruption
    - Information leakage which is illegal or embarrassing
  - Target Date – 3 weeks

# 4 Risk Categories (contd)

- **Moderate**
  - Examples
    - Confidential issues in user information
    - Local DoS
    - Potentially serious, but hard to exploit problem.
      - *E.g. hard to exploit buffer overflow*
  - Target Date = 3 months
- **Low**
  - Examples
    - Small system information leak
    - Issue which is only exploitable in unlikely circumstances, or where an exploit cannot be found
    - Issue where impact on service minimal
  - Target Date = 6 months

# What we don't do

- **Fix software ourselves**
  - Although some members are also involved in the software development so do fix software
  - Not a GSVG task
- **Fix 3rd party software or expect EGEE-II to fix 3rd party software**
  - Bug manager contacts the 3rd parties to arrange a fix
- **Pass on information to individual sites**
  - Operational issues
    - OSCT passes appropriate info onto sites
  - Bug fixes
    - EGEE broadcasts when a release is made
    - release note refers to advisory
  - People at sites may subscribe to advisory subscription list when we get it running
  - But we are friendly enough and try to answer questions!
- **Publicise information on 3rd party software without permission from the 3rd party**
- **Handle incidents**
  - We attempt to help prevent incidents by getting vulnerabilities fixed

# What is going well

- **Principle is now well accepted**
- **Processing shortly after issues are submitted working well**
- **RAT carrying out good Risk Assessments**
- **Writing advisories**
  - Starting to put them on web page
- **Starting to release information on the TD even if a fix is not available**
- **Contact and relationships with other parties**
  - Especially SA3, JRA1, and OSCT

# Public disclosure agreed!

- **Started in 2005**
  - Initially some didn't want a vulnerability activity
  - Attitude was 'if we produce a list of possible problems, sysadmins will want it, then they might not want to install software'
- **The GSVG deliverable (DSA1.3) approved by the EGEE PMB and accepted by the EU**
  - Stated that for EGEE/glite s/w we will release advisories on the Target Date
  - Starting to do this
  - Getting the work approved and process accepted has been a long haul

# Disclosure Policy and Target Date

- **By carrying out Risk Assessments and setting a TD we are allowing the resolution of issues to be prioritized**
- **The TD can also be seen as the maximum length of time the issue can be lived with, without taking action**
- **On Target Date, information on the issue is made public**
  - Regardless of whether a fix is available
  - This only applies to EGEE software
- **This is to ensure confidence in the system**
  - People less likely to discuss issues on public mailing list rather than use our system
- **Public disclosure ensures all those who install the software have access to information on known vulnerabilities**

# Some numbers (28rd Sept 2007)

- **122 issues entered since we started in 2005**
- **62 open (42 s/w bugs, 19 more general, 1 in assessment)**
- **60 closed (25 bug fixes, 7 operational, 6 general, 17 invalid, 5 duplicates)**
- **Risk – all those fully assessed with EGEE-II criteria**
  - 1 Extremely Critical, 9 High (2 open), 11 Moderate (8 open), 17 Low (14 open)
- **Risk – all open s/w bugs**
  - 2 High, 8 Moderate, 14 Low, 2 not applicable, 18 Pre-EGEE2, 1 awaiting assessment

  Pre-EGEE2 sites informed according to pre-EGEE2 process
- **So far put 15 advisories on web (11 past TD but no patch)**

# Not perfect – but improving

- **Processing when issues fixed**
  - Finding that some have been fixed but advisory not included in release notes
  - If sites are keeping software patched, some patches fixed vulnerabilities which didn't get advisories included in release notes
  - Changed system a little and working well with SA3
    - release notes should point to advisory
    - release notes include affected modules and any installation info
    - advisory refers to "Release"
- **Some issues not getting fixed by the Target Date**
  - Now we are putting out the advisories on the web page.
  - Some have been around for a long time
- **Some see GSVG as a bit of a 'black hole'**
  - Hopefully this will improve as we are now putting advisories on the web page

# What still needs improvement

- **Some issues not a simple software bug**
  - May require re-design, and/or a major addition to functionality to fully address
  - Can't simply ask developers to patch
  - Most problems that have been in database for a while are well known
- **Solutions need to be sought between TCG, SCG, and others**
- **Recent example – glexec concerns**
  - There are concerns about whether the design/principle is appropriate and complies with policy
- **This is main area that needs improvement**
  - issues that have been in the system long term tend to be this type

# Main areas that are not simple bugs

- **Authorize all actions**
  - ensure Authorization cannot be bypassed
  - include file and information access
    - Confidentiality is a big concern for some applications
  - several issues due to lack of R-GMA authorization
    - both for read and write
    - in development
- **Ensure model/design is secure and complies with policy**
  - Not a specific ‘bug’
  - New EGEE security Architect

# Main areas that are not simple bugs (2)

- **Grid wide quota system is needed**
  - Per user, per VO
  - Processes, file space etc per WN, Per site..
    - Prevents DoS from overload
  - And globally
- **Better logging**
  - More efficient incident handling
    - Requirement to trace original DN
  - Useful for users too
  - In work
    - https://twiki.cern.ch/twiki/pub/EGEE/EGEEgLite/logging.html

# Main areas that are not simple bugs (3)

- **VO code and Middleware code integrity**
  - Ensuring sites install ‘real’ code
  - Users/VOs being able to ensure that when they run a job it is using code as expected
  - Software signing?
- **Restricting outbound access**
  - Prevention of Grid being used to attack other systems

# Developers guidelines

- **Wish to minimize introduction of new grid security vulnerability issues in the code**
- **In 2005 produced a document including a checklist for developers**
  - http://www.gridpp.ac.uk/gsvg/docsguides/GridPPVulnerability.pdf
- **Tended not to be used, developers have too much to do, was probably too long**
- **Change to a list of 10-20 top things to watch out for e.g.**
  - several vulnerabilities are simple file permissions
    - Both middleware developers and those producing yaim configuration files need to ensure file permissions are set correctly
  - checking input – avoiding SQL injection and XSS vulnerabilities
  - Still get buffer overflow vulnerabilities
  - ISSeG started on this – possible collaboration

# What have we learnt?

- **Vulnerability handling is a sensitive area**
  - hard to get agreement on what we should do
- **Even when we agree in principle what should be done, it is a lot harder to actually do it**
  - Everything takes far longer than expected
- **Non-trivial getting processes working well with multiple parties involved in different institutions**
- **Keep things as simple as possible**
  - Tendency to make things too complicated
  - Easy to get bogged down trying to define how to cope with each type of issue and situation
  - Have a few basic cases, then use some common sense with those that don't quite fit

# More info

- The Grid Security Vulnerability Group webpage is at http://www.gridpp.ac.uk/gsvg/

# Questions

- ??