# The Grid Security Vulnerability Group Activity in Central Europe in EGEE II

***Kálmán Kővári,***

***IT-Services Hungary Ltd, RMKI-KFKI, Loránd Eötvös University Budapest (ELTE)***

*Bratislava, 29th April 2008*

*(Based on Linda Cornwall's EGEE'07 presentation with some updates)*

# Contents

- Role of the Grid Security Vulnerability Group (GSVG)
- Setup and people involved
- GSVG process and Strategy, Risk Assessments
- Activity with numbers
- Summary
- Time for Q&A

# Role of GSVG

- **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 )

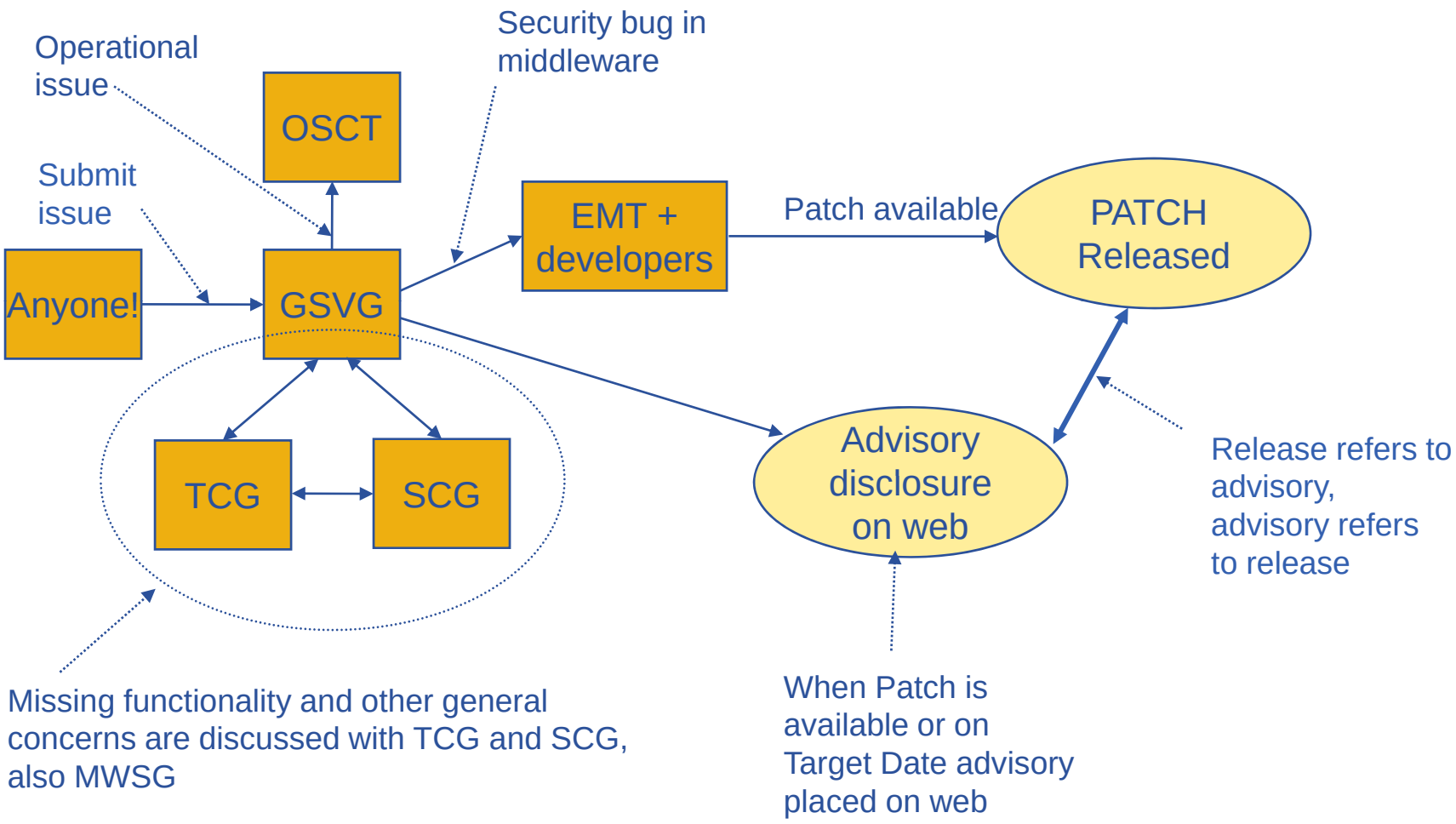
# Process and strategy in EGEE-II – to first order

- **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



# 4 Risk Categories

- **Extremely Critical**
  - Examples
    - Trivial Grid Wide DoS with no Credentials
    - 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

# 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 (10th April 2008)

- **133 issues entered since we started in 2005**
- **55 open (39 s/w bugs, 16 more general)**
- **78 closed (soon we close about 12 more when glite 3.1/code in head fully rolled out.)**
- **Risk – all those fully assessed with EGEE-II criteria**
  - 1 Extremely Critical, 11 High (2 open), 15 Moderate (9 open), 19 Low (14 open)
- **Risk – all open s/w bugs**
  - 2 High, 9 Moderate, 14 Low, 2 not applicable, 12 Pre-EGEE2, 2 n/a (software not yet certified)
  - Pre-EGEE2 sites informed according to pre-EGEE2 process
- **25 advisories put on the web since July 2007**
  - Before then advisories were included in the release notes

# Not perfect – but improving

- **Processing when issues fixed**
  - During mid 2007 we found 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 this is working well with SA3
    - release notes 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 in the past have seen 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
  - Problems that have been in database for a while are well known
- **Solutions need to be sought between TCG, SCG, and others**
- **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

# 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**
- **Suggest 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

# 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

# Where further?

- **Security awareness rose recently**
  - No grid abuse yet reported
  - Goal is to keep it up in long term
- **Lately code reviews have created proactive issues:**
  - Some SQL injection issues revealed
  - Some false library links corrected
  - Still ongoing, results have proven worth the effort
- **All the recent activities are to be continued in EGEE-III**
  - 2-3 New partners expected to contribute manpower to GSVG
- **We have reached a certain maturity, efficient level of work**
  - We provide a reliable service to developers and sysadmins
  - Still some need to fine tune processes between the various group
  - Have to stay reliable, that needs manpower still

# For EGEE-III

- **GSVG should be more active in suggesting general ways to improve security**
  - e.g. software signing

# More info

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

- **Time for discussion!**