GSVG issues handling

Dr Linda Cornwall CCLRC (RAL)

SA1 Security meeting, EGEE06, Sept 2006

Contents

- Vulnerability Task in EGEE II
- Setup of the GSVG in EGEE II
- What we do – to first order
- Disclosure policy in EGEE II
- Risk Assessments
- Process

The Vulnerability Task in EGEE II

- **In EGEE II there is manpower for the "Grid Services Security Vulnerability and Risk Assessment" Task ☺**
- **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
- **Handling of Vulnerability issues is the largest activity in this task**
  - Which deals with specific issues

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 week
  - At present 4 members
- **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**

What we do - to first order

- **Issue is submitted**
  - Anyone can submit an issue
- **At least 3 RAT members carry out a Risk Assessment**
- **Target Date (TD) set according to Risk**
- **Mirror bug entered in JRA1 Savannah**
- **The issue is then in the hands of JRA1/EMT**
- **EMT co-ordinates fixing the issue and the release**

Disclosure Policy for EGEE II

- **We want to move to a responsible public disclosure policy**
- **On Target Date, information on the issue is made public**
  - Regardless of whether a fix is available
- **This depends on management approval,**
  - We need to prove we can do good Risk Assessments

Risk Assessments

Issues divided into 4 categories of risk

- Extremely Critical
- High
- Moderate
- Low

Extremely Critical

Examples

- Trivial compromise of core grid component
- Remotely exploitable issue that can lead to system compromise
- Root access with no Credentials
- Trivial Grid Wide DoS with no Credentials
- Trivial use of the Grid to launch an attack on other systems with no credentials

- Target date – 2 days
- Alert OSCT and EMT immediately
- Expectation – Very rare if ever

High Risk

Examples

- Remote exploit against middleware service
- Spoofing – carrying an action on someone's behalf
- Exploit against MW component that gives elevated access
- Grid-wide DoS
- Information leakage which is illegal or embarrassing

- Target Date 3 weeks

- Expectation – small number

Moderate

Examples

- **Confidential issues in user information**
- **Local DoS**
- **Potentially serious, but hard to exploit problem.**
  - E.g. hard to exploit buffer overflow
- **Race conditions that are hard to exploit**

- **Target Date 3 months**

Low

Examples

- Small system information leak
- Impact on service minimal

- Note – if 2 low risk issues could produce problem, this should be entered as a higher risk issue

- Target Date – 6 months

Notes

- **If anyone thinks an issue is extremely critical – all available RAT members should look at it**
- **Other than that vote –**
  - E.g. If 3 look initially, and 2 say moderate, 1 low – set as moderate
- **The Risk classification could change**
  - Rise if information is available publicly or issue has been exploited
  - Fall if more information comes to light, e.g. part of the code not aware of mitigates problem
- **Formula for setting TD is not for the RAT to decide unilaterally**
  - We have proposed 2 days 3 weeks 3months 6months
  - Need to agree with management

Issues arising from missing functionality

- **If these are entered we will carry out risk assessment**
- **But handle differently**
  - Inform TCG of what we consider to be the risk
  - But not set TD

Advisories

- **Advisory on issue is partially written when the risk assessment is carried out**
  - By the RAT member the issue is allocated to, consulting other RAT members (if necessary) and appropriate developers
  - Mostly just a few sentences
  - Then passed to EMT for completion
- **Advisories available publicly on Target Date (or earlier if fix is available)**
- **Advisories should be included in the release notes**
- **Advisories should include what to do (completed by EMT)**
  - Solution – will need to be completed by those releasing the software
  - Patch/work around – which may reduce the service functionality
  - In worst case – advice to stop a service
- **Advisories will not describe how to exploit issue**

Examples

- We have carried out Risk Assessments on 8 sample issues
- We believe these demonstrate that we can categorize issues appropriately

Process(1)

- Issues reported (usually by e-mail)

Then Core group member

- Enters issue into Grid Vulnerability Savannah
- Acknowledges reporter with a standard letter
- Sends E-mail to RAT asking for Risk Assessment

Process (2)

The Risk Assessment Process is carried out by the RAT

- **Facts are checked with appropriate developers + with reporter (if appropriate)**
  - JRA1 leaders may be asked if we don't know who the appropriate developers are
- **Risk Assessment Carried out, i.e. Risk category established**
  - at least 3 RAT members should look at each issue
- **Advisory partially written by RAT**
  - Just a few sentences
- **Then RAT advises core group member the Risk Assessment has been carried out**

Process (3)

Then issue is briefly handled by core group

- **If extremely critical – EMT, OSCT informed immediately**
- **Target Date Set according to Risk**
  - Fixed formula
- **JRA1 Savannah mirror bug entered with TD in text**
  - Set to critical if high risk or extremely critical
  - Set to normal if moderate or low risk
- **Standard mail sent to reporter informing them of the completion of the risk assessment, and the Target Date**
- **Issue allocated to JRA1**
- **John White, Claudio Grandi, and Oliver Keeble informed by e-mail**

Process (4)

- **Then it is out of the GSVG hands – it is up to JRA1/EMT/SA3 to handle the issue and ensure the advisory is issued on time**
- **This includes answering further questions from the reporter**
  - Note that the reporter should receive the advisory

Other notes

- We aim to carry out Risk Assessments within 2 working days of an issue being submitted
- We can make no guarantees, while we have more effort than prior to EGEE II effort/availability of core group people/RAT people cannot be guaranteed

Request for approval

- We believe we have an adequate process and strategy for carrying out Risk Assessments,
- We are ready to request approval for full public disclosure, i.e. making information public on the Target date regardless whether it has been fixed

Issues already present

- In the past we carried out less rigorous risk assessments, and passed information to LCG Security Contacts
- We need to re-visit the 60 or so issues still open
- Some are reminders like “test systems need to be secure”
- Some have been fixed in the software, ‘awaiting release’
- Some still need a proper risk assessment
- We will work our way through these issues using the new strategy as soon as possible

Questions/Discussion