Grid Security Vulnerability Group

Linda Cornwall, GDB, CERN
7th September 2005

L.A.Cornwall@rl.ac.uk

CCLRC

Introduction

- Current grids
- Logging and tackling specific issues
- The vulnerability group
- Process
- Current state
- Questions? Project approval?

Current grids

- Grid Middleware has been written during the previous few years and other software has been used in various innovative ways to enable functional grids to be deployed
- Emphasis has been on functionality
- A lot has been achieved
- Grids are not perfect, there are problems that could be exploited (mostly by people with credentials)
- Up to now we have had a very friendly co-operative environment, hackers have not been very aware of us

Logging and tackling specific issues

- This is a sensitive issue
  - There has been a reluctance to write anything down because sysadmins will rightly want info, some want the info to be made available publicly, and then may not want to install the software
- We can't fix everything quickly, we know that
- We want to tackle the problem as a collaboration between all parties, including developers, system administrators and management
- We want to ensure grids become more secure and keep them deployed
- We do not want any incidents

Vulnerability Group

- We have formed a vulnerability Group to tackle specific vulnerability issues
- This group is a collaboration between members of the project with useful knowledge or experience – including both system administrators and developers who want to see improvements in Grid Security
- Grid Vulnerability Savannah is set up
- Mailing list is available

Aim of Vulnerability group

- The aim of the group is to improve the quality of our software and deployment and protect our sites
- Inform developers (and their managers!) of vulnerabilities as they are identified, and encourage them to produce fixes or reduce their impact
- Inform security contacts as appropriate
- Aim is to keep grids deployed, keep appropriate people informed, not inform potential hackers, and fix problems
- This is not for incidents – if a vulnerability has been exploited it is handled by incident response
- Can be seen as incident prevention

Vulnerability organisation (1)

- Vulnerability group
  - Members have read and write access to the Savannah grid vulnerability project
  - Members log any problems they become aware of in the Grid Vulnerability Savannah
    - logged as bugs as that is what Savannah does, but should really be considered to be vulnerability issues not bugs
  - Non members may submit bugs, and they should receive feedback, but they may not read the database
  - Members may be members of the Grid vulnerability mailing list – which means they may write to the list. (It is not archived publicly)
  - Problems or potential problems may be discussed on the mailing list

Vulnerability Organisation (2)

- Vulnerability Core
  - Manage membership of the vulnerability group
  - Ensure that appropriate people take responsibility for dealing with vulnerabilities
    - Developers
    - Deployment people (at present security contacts list)
    - Appropriate people to carry out risk assessments

Vulnerability group members

- Ask to join
- Sysadmins and developers in LCG, EGEE, GridPP are entitled to join
  - Others at discretion of the core group
- Are known (first or second hand) to a member of the vulnerability core or their affiliation can be checked (e.g. on the GOC database)
- At present 35 members

Process

- Someone enters a vulnerability
  - If it has been exploited escalate immediately to incident response
  - Should not really be entered in the vulnerability base
- If urgent action is needed
  - e.g. an urgent change in the configuration, or to turn a system off
  - Inform security contacts (OSCT will define who is best to contact later)

Process (2)

- Initial assessment
  - If there is an EGEE software problem
    - Assign bug to appropriate member of group
    - Define a target time for fixing the problem
    - Enter a reference bug in jra1 savannah with no details
  - If there is a problem with an external package
    - inform as appropriate for that package
  - If an action is needed (e.g. configuration change)
    - If urgent – inform security contacts
    - Otherwise deal with as part of the EGEE deployment procedures

Process (3)

- If a solution is available
  - Handle through EGEE deployment procedures
- If solution unlikely to be available by target time
  - Carry out a detailed risk assessment
- If target time is reached and no solution is available
  - Pass on description and risk assessment to security contacts
  - This will be passed on to sysadmins
  - No publication by ourselves on a public web page
  - We have internal knowledge of EGEE middleware, we cannot take the same approach as e.g. CERT/CC and make knowledge public when target time has passed
  - JRA1/EGEE can make it public if they think it is appropriate

Progress web page

- We plan to have a web page accessible with a certificate and possibly VO membership
- For each vulnerability bug
  - Some sort of title indicating what package is involved (but no details)
  - Which group is responsible
  - Due date
  - When fixed
  - When not fixed by due date
- This flags progress
- This flags groups that are not fixing bugs

Current status

- Mailing list is available
- Grid vulnerability Savannah is set up (42 ‘bugs’)
  - Reminder - ‘bugs’ should be read as ‘vulnerabilities’ – only called bugs because that is what Savannah does
- Not much happened with so many on holiday in August
- Not yet set target times, done much analysis, entered ‘mirror’ entries in JRA1 savannah
- Need some effort
  - Especially for risk analysis

Current entries

- Of the 42 ‘vulnerabilities’, from initial look
- 20 are only exploitable by an authorized user
- 3 Authenticated user
- 2 people with access to grid machines
- 12 less well defined e.g.
  - vary from needing to install a rogue CE
  - warnings of consequences if certain machines hacked
  - Ability to set short password
- 5 No credentials (2 considered major)
  - 1 in general to take steps against DOS
  - 1 can be made much less of problem by a configuration change

Project agreement

- Approach agreed at the EGEE conference in Athens.
  - agreed that we will form this group and take this approach
  - Developers and deployment people present
- Also supported by the JRA1 meeting in Brno
- We are seeking formal management approval LCG, EGEE, GridPP
  - To cover ourselves (concerns about liability)
  - To ensure fixing the vulnerability bugs gets sufficient priority

Notes

- This is best efforts work
- We need management to give this priority
  - EGEE developers to fix problems
  - Appropriate people to carry out risk analysis
  - Otherwise nothing will happen
- We are not doing Security operations
  - OSCT should decide who to pass info onto if an urgent change is needed
- We will probably improve the process later
  - Try it out, and improve with time

To Join

- e-mail myself to join the e-mail list
  - L.A.Cornwall@rl.ac.uk
- Request membership of the Grid Vulnerability Savannah by logging onto Savannah
  - https://savannah.cern.ch/projects/grid-vul/

Discussion

- Any questions?
- Is the Grid Deployment Board able to approve our policy and approach?