Handling Software Vulnerabilities

Dr Linda Cornwall, STFC,
Rutherford Appleton Laboratory

GridPP
UK Computing for Particle Physics

e-infrastructure

Contents

- Background
- The Purpose of EGI Software Vulnerability Group (SVG)
- What is a Software Vulnerability?
- Handling Software Vulnerabilities
- Time for questions

Issue handling background

- It was recognised in 2005 that vulnerability handling in the Grid environment was important
- Started logging vulnerabilities, and encouraging people to fix them
- Included the Grid Security Vulnerability Group (GSVG) in EGEE-II and EGEE-III
- GSVG Issue handling process developed in 2006
  - Mostly concerned gLite
- 193 vulnerabilities reported

  ~100 fixed, rest invalid/duplicate/operational/obsolete

Purpose of the SVG

May 2010 the EGI Software Vulnerability Group started – purpose:

"To eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware, prevent the introduction of new ones and prevent security incidents".

Changed situation for EGI

- In EGEE – grid middleware was largely developed within the EGEE project
  - GSVG focussed on gLite
- In EGI software is mostly developed outside the EGI project
- Middleware is to be distributed by EGI as the Unified Middleware Distribution (UMD)
- Much of the software in the UMD is provided by the European Middleware Initiative (EMI) project

Changed situation (2)

- Increased Scope, not just gLite
  - All EMI software - gLite, ARC, Unicore, dCache
  - Plus IGE (Initiative for Globus in Europe)
- Much of the EGI SVG process for handling vulnerabilities is based on the GSVG process and what was learnt

Why is SVG in EGI?

- SVG is in EGI foremost to try to ensure that the software used in the deployed EGI infrastructure is as secure and free from vulnerabilities as possible.
  - It ensures a process exists for handling vulnerabilities in Grid Middleware distributed by EGI in the UMD
  - It reduces the operational cost if the risk from vulnerabilities can be mitigated
  - It is recognised that the infrastructure will never be perfectly secure

What is a vulnerability?

- A weakness allowing a principal (e.g. a user) to gain access to or influence a system beyond the intended rights
  - Unauthenticated or Unauthorized user can gain access
  - User (authorized or not) can
    - gain unintended privileges – e.g. root or admin
    - damage a system
    - gain unintended access to data or information
    - delete or change another user's data
    - impersonate another user

What is not a vulnerability

- Actions which can only be carried out by site administrators
  - Site administrators mostly trusted
  - Except with bulk encrypted data + keys
- Issues which provide information that may be useful to an attacker
  - Not usually treated as vulnerabilities
- General concerns
  - e.g. “this may not be installed correctly”

3 main activities for reducing vulnerabilities

- Handling vulnerabilities found/reported
  - This is the main activity
- Assessing software for vulnerabilities
  - Some done by SVG, some by other groups
  - Generally treated in the same way as other vulnerabilities reported
- Preventing new vulnerabilities being introduced
  - Developer education, awareness

SVG membership

- SVG membership comes from various sources
  - Software providers
    - gLite, ARC, Unicore
  - EGI CSIRT team
    - The computer Security Incident Response Team who strive to ensure that the deployment is as secure as possible
  - Sites and NGIs
- Most in Risk Assessment Team (RAT)
  - Handle vulnerabilities reported

Current RAT members

Linda Cornwall (RAL)
Krzysztof Benedyczak(UWAR) (Unicore)
Stephen Burke(RAL)
Vincenzo Ciaschini(INFN) (gLite)
Sven Gabriel (Nikhef/FOM) (CSIRT)
Oscar Koeroo (Nikhef/FOM) (gLite, IGE contact)
Daniel Kouril (CESNET) (CSIRT, gLite)
Maarten Litmaath (CERN) (gLite)
Mingchao Ma (RAL) (CSIRT)
Leif Nixon(NORDUNET) (CSIRT)
Eygene Ryabinkin(RRC-KI) (CSIRT)
Mischa Sallé (Nikhef) (gLite, IGE contact)
Åke Sandgren(HP2CN) (CSIRT)
Bernd Schuler(JUELICH) (Unicore)
Steve Traylen(CERN)
Anders Waananen(UCPH) (ARC)

Issue handling process

- Issue handling carried out by the EGI Risk Assessment Team (RAT)
  - 16 members
  - Have access to the vulnerability information
- Anyone may report an issue
  - By e-mail to

  report-vulnerability@egi.eu
- Issue is investigated by a collaboration between the RAT, reporter and developers.

Issue handling (2)

- If the Issue is valid, the RAT places it in one of 4 risk categories

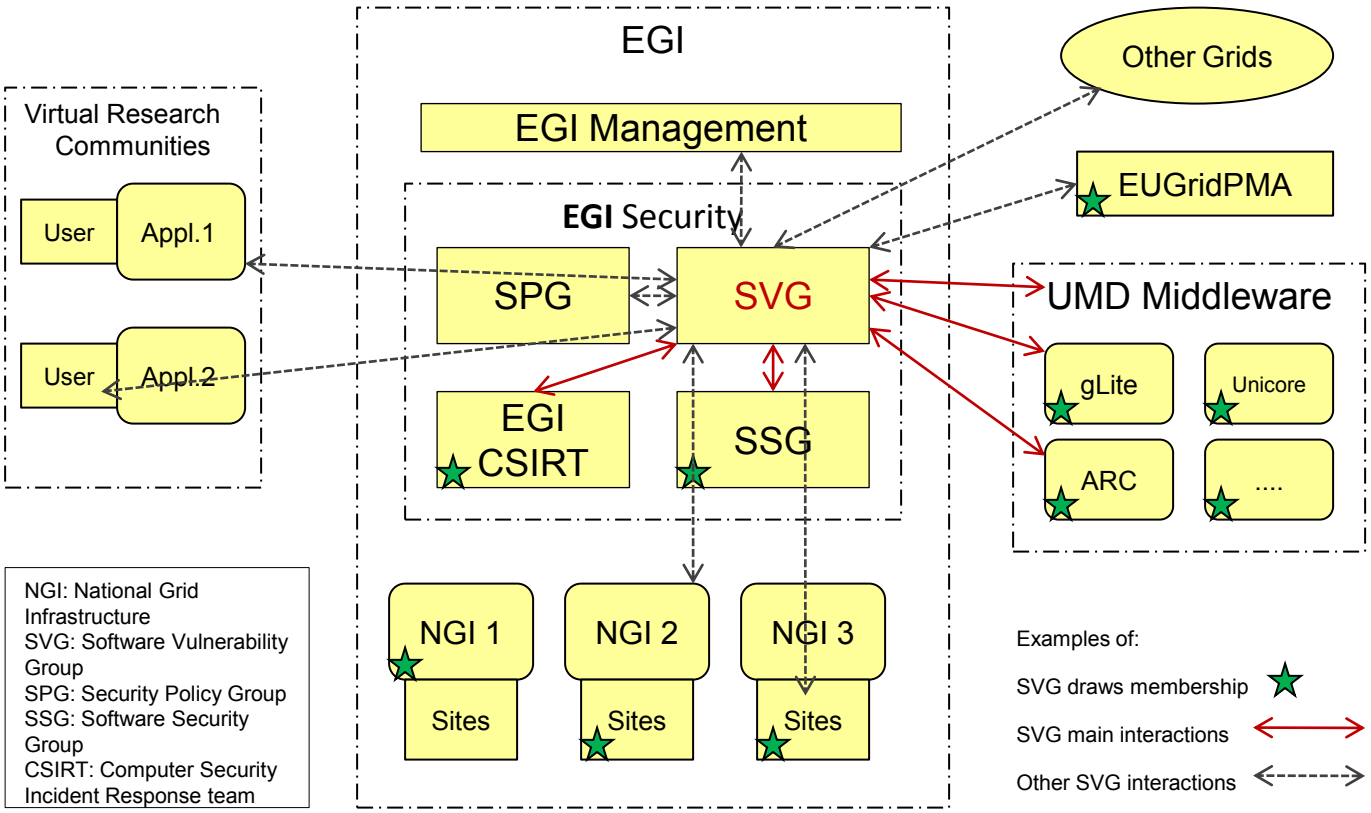
  Critical, High, Moderate or Low

- Target Date for resolution set according to the Risk
  - Critical - 3 days, High - 6 weeks, Moderate – 4 months, Low - 1 year
  - Aim to reach this point within 4 working days
    - Within 1 day for critical issues
  - This allows the prioritization of the timely resolution of issues according to their severity

Issue handling (3)

- It is then up to the developers and release team to try and fix the problem by the Target Date or earlier
  - All relevant parties then get to access the info
  - SVG will provide help and advice if appropriate
- Advisory issued when patch is available or on Target Date – whichever the sooner
  - This is known as responsible disclosure
  - Advisory refers to release notes, release notes refer to advisory
  - Advisory sent to site-security-contacts and NGI-security-contacts

Interaction with others



Software providers agree to SVG process

- Service Level Agreements (SLAs) between Software Providers (EMI, IGE etc) and EGI mean that the issue handling process is accepted
  - Agree to provide contact details, response times
  - Agree to attempt to fix in time for Target date
- Providers participate in SVG

Types of Software

- System largely set up to handle vulnerabilities in software distributed in the EGI Unified Middleware Distribution (UMD)
  - No other handling process
  - EGI has an SLA with these providers
- Vulnerabilities in other software may be reported
  - SVG will pass the information on
  - SVG may provide a Risk Assessment for EGI

Other software

- If the software is not grid middleware (e.g. Linux) – generally 2 situations:

1. Someone becomes aware of a vulnerability that has been fixed by the provider
   - Most common case
   - SVG and (mainly) CSIRT consider risk/urgency of upgrade in the EGI environment
2. Someone finds a vulnerability not known by provider
   - Information passed onto appropriate parties. SVG and CSIRT again consider the Risk

Notes on Risk

- The EGI through SVG has established a structured and formal approach to assess risk
- The RAT considers the risk – as mitigating or aggravating factors may exist in the Grid environment
- The RAT usually agrees on the category
  - We say we vote
  - Consensus is the norm

Critical issues

- A special process is carried out
- This includes alerting all concerned (CSIRT, EGI Middleware unit, developers)
  - Consider whether it is possible to produce a patch in a short timescale
  - Whether a longer TD should be set
  - Whether mitigating operational action should be carried out
  - Inform sites what should be done
- EGI CSIRT critical vulnerability handling procedure is carried out when solution available

Reporter View

- The reporter must NOT
  - Discuss on a mailing list – especially one with an open subscription policy or which is archived publically
  - Post information on a web page
  - Publicise in any way without agreement of SVG
- The reporter SHOULD report to SVG via

  report-vulnerability@egi.eu

Reporter View (2)

- The reporter will receive acknowledgement when an issue is reported
- The reporter should help and co-operate with investigation
  - Not mandatory – but would be good
- The reporter will receive information, including the advisory

Reporters view(3)

It doesn’t matter if a user or site admin reports something to us which turns out to be operational or a configuration problem – CSIRT members are in the RAT and will see the issue

Sites and NGIs view

- Sites should install up to date software
  - (this is stating the obvious to this audience)
- Sites should report any vulnerabilities they find
- Site security contacts should receive notification of when vulnerabilities are fixed
  - i.e. Advisories

Current status

- Infrastructure transferred to EGI (RT, wiki)
- Templates etc. in place
- Established the contact details with various parties
  - SW providers, packagers etc.
- 33 issues reported (15 grid middleware)
  - 5 released, 6 (Low) in EMI-1, 4(Low) not simple bugs,
  - rest non MW/duplicate/invalid
    - some needed action, not work free!
- Process running fairly smoothly

Other changes for EGI

- Closer collaboration between EGI SVG and CSIRT
  - Several CSIRT members are in the SVG RAT
  - Joint discussion on some of the ‘What to do’

More information

- Vulnerability Issue handling Process as part of Operational Security Procedures milestone MS405 https://documents.egi.eu/secure/ShowDocument?docid=47
  - New version due end July 2011
- Web page https://wiki.egi.eu/wiki/SVG
- Poster “Software Vulnerability Group” https://wiki.egi.eu/wiki/File:PosterSVG-2011.pdf

Questions?

- ??