Recent Experiences in Operational Security:

Incident prevention and incident handling in the EGI and WLCG infrastructure

Dr Linda Cornwall, STFC.

HEPiX Spring 2015

WLCG and EGI

- The (Worldwide) LHC Computing Grid and The European EGI Infrastructure share a lot of the same resources
- Also share Security teams and activities

Contents

- Incident Prevention
  - Policy definition
  - Vulnerability handling
  - Security monitoring
- Incident handling and incidents from the last year
- Evolving the work

Security Incident Prevention

- Far more work goes into preventing incidents than handling them
  - Security Policy definition
  - Software Security, especially Software Vulnerability handling
  - Security monitoring - monitoring for known vulnerabilities

Security Policy Definition

- Security Policy definition is carried out by the EGI Security Policy Group (SPG)
  - Defines the behaviour expected from NGIs, Sites, Users, VOs and other participants to maintain a beneficial and effective working environment
- Output is various policy documents
  - Parties read and sign, so that they know and understand what they should and should not do

Software Vulnerability Group message – if you find a vulnerability

If it is NOT public knowledge

- DO 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
- DO report to SVG via

  report-vulnerability@egi.eu

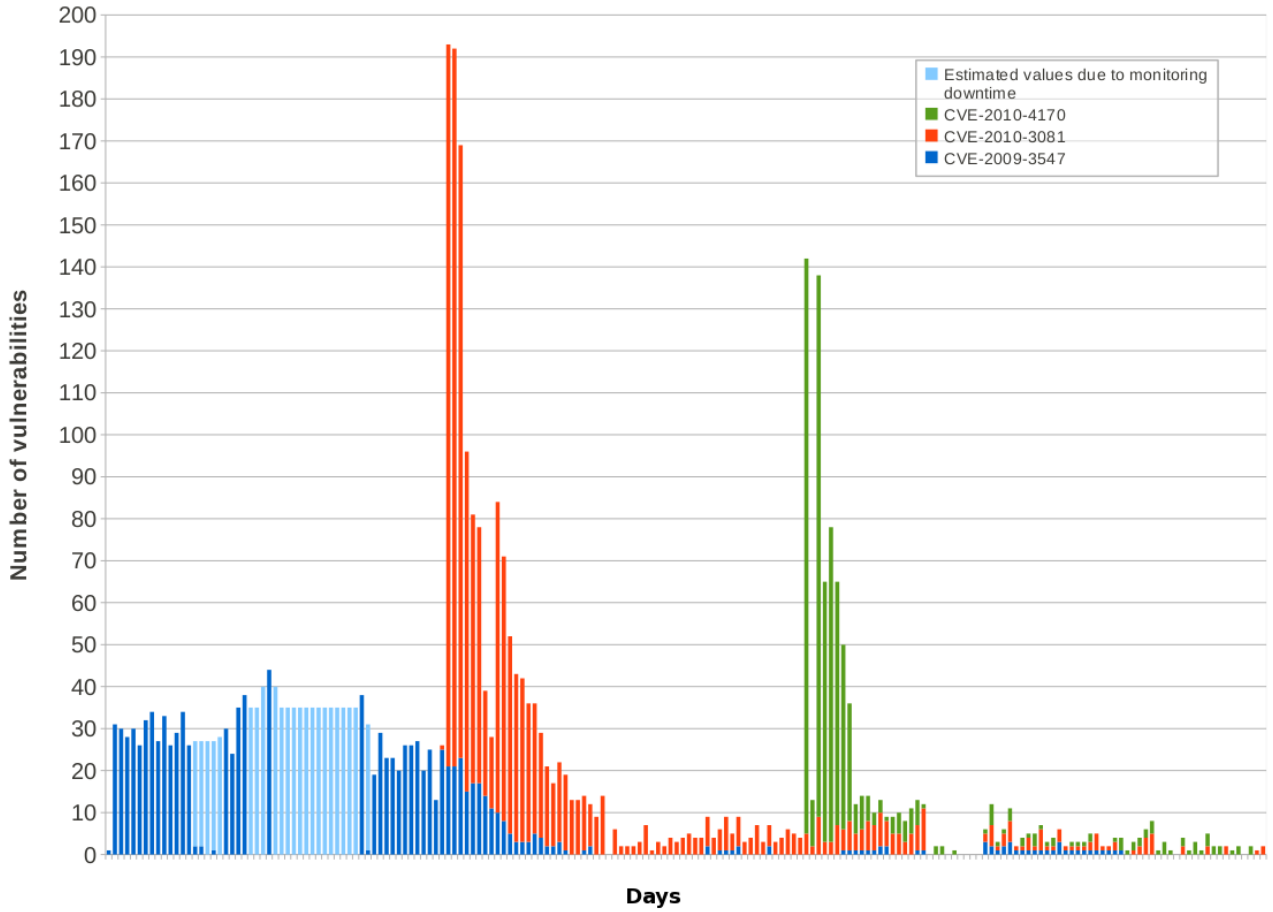
Software Vulnerability Handling – Approved Procedure

- If it has not been announced, SVG contacts the software provider and the software provider investigates (with SVG member, reporter as appropriate)
- If relevant to EGI, a risk assessment is carried out
  - Critical, High, Moderate, Low
- If not fixed, Target date for resolution set according to risk
  - Critical 3 days (special process), High 6 weeks, Moderate 4 months, Low 1 year.
- Advisory issued, if/when fixed or on Target date whichever is the sooner.
  - (High and Critical only if 'announced')
- For 'Critical' vulnerabilities sites must patch in 7 days.

High and Critical Vulnerabilities monitored

- Sites are monitored for ‘High’ and ‘Critical vulnerabilities
  - In last year 5 new critical, 16 High
- EGI CSIRT chases sites which are exposing ‘Critical’ vulnerabilities
  - For new vulnerabilities sites are given 7 days to patch or face suspension (2 days older)
- Respond if asked to by IRTF/CSIRT
  - The threat of site suspension has reduced the time sites are exposed to ‘critical’

Time taken for sites to patch – courtesy of Daniel Kouril



Incident Handling – according to approved procedure

- If you find or suspect an incident at your site report to:--
  - abuse@egi.eu
  - Your NGI security contact
  - Your Local institute security team
- Don’t power off the system
- Disconnect from the network if you can
- The EGI CSIRT team will help you investigate
- Fortunately there are not many incidents
  - Incident prevention is quite successful.

Emergency (User) suspension

- It is now possible to suspend a User (DN) across the whole infrastructure via ARGUS
- This may be done in the case of an incident where a DN is implicated
  - E.g. user has mis-used resources
  - Potentially compromised DN
- This is not 100% working yet
  - Some sites not implementing yet
  - Some types of SE's not working yet.
  - We need to get this 100% working

Incidents during last year (8)

- Primecoin mining (Policy violation)
- Open Hostkey leaking private information
- User cert mis-use
- Fed Cloud incident
  - Due to bad endorsed VM
- UI compromised (4 user IDs compromized)
- Shellshock related compromises to Perfsonar nodes (multiple sites)
- Compromise due to a port being left open
- DDoS to some EGI services

Security Training and challenges

- EGI CSIRT provides security training to site administrators and others
  - E.g. last week at the ISGC in Taipei
  - This includes some hands on forensics training
- EGI carries out security challenges
  - Challenges to sites with ‘mock’ incidents
  - This year confined to contact challenges

EGI CSIRT now Trusted Introducer certified

Evolving the Security Work

- Evolving the security work is necessary due to e.g.
  - The EGI federated Cloud
    - Changing responsibility model - this has a major impact in incident response
    - Changing technology
  - Long Tail of Science
    - Different trust model

Have some EU H2020 funding for 'EGI engage' to carry out this evolution

Policy documents revision

- Getting rid of ‘Grid’
  - Policies apply to all technology and services
  - E.g. Acceptable use policy
    - External draft – request for feedback and comments
- Data Protection Policy
  - Formerly only had “Grid Policy on the handling of User Level Job accounting data
  - Finding Data protection policy needed as User level data is being monitored and exposed inappropriately.

Vulnerability handling evolution

- Now more software is coming into use where SVG members have no knowledge – solutions include:--
  - New members of SVG who know about cloud software, especially tools written within the community
  - ‘Expert’ contact for all software Cloud enabling software deployed in the Fed Cloud
  - VO software – assume VO security contact is responsible and know who to contact
    - No more than 2 steps to the right person.

Software security checking

- For some community cloud enabling software have a detailed ‘Technology provider’ questionnaire
- For other software propose something simpler:--
  - License details
  - How long will it be under security support?
  - How are security problems reported?
  - Are security problems announced?
  - Check compliance with Data Protection policy
  - Some other simple technical checks – e.g. is user input validated, bad constructs – not obviously bad

‘Security Threat risk Assessment’

- Security Threat Risk Assessment carried out in 2012
  - Based on the EGI Deployment as it was then – and other concerns
- Threats scoring high risk value included:--
  - New software or technology may be installed which leads to security problems (Highest value)
  - The move to more use of Cloud technologies may lead to security problems
- Plan to carry out another assessment, based on the EGI Federated Cloud.
  - Based on a written down situation as we understand it, and agreed with the EGI Fed Cloud team
  - This will allow us to identify where the highest risk threats are and address them

Questions??

Links

- List of policy docs at

https://wiki.egi.eu/wiki/SPG:Documents

- New Acceptable Use Policy

https://wiki.egi.eu/wiki/SPG:Drafts:Acceptable_Use_Policy_March_2015

- EGI Software vulnerability handling procedure

https://documents.egi.eu/public/ShowDocument?docid=717

- Approved Incident handling procedure

https://documents.egi.eu/public/ShowDocument?docid=710

- Security training example (Taipei March 2015) http://indico3.twgrid.org/indico/sessionDisplay.py?sessionId=43&tab=time_table&confId=593#20150315