SVG Collaboration and Coordination in EOSC

Linda Cornwall (STFC)

CSIRT F2F CERN Jan 2018

Contents

- In Helsinki I described SVG
  - Described how we do things
  - Updated procedure last year
  - I can re-show some of those slides if people wish
- Today I'm focussing on what has happened since, and how we can go forwards
  - To start a discussion
- First a few updates
- Then mainly ideas for what to do

Numbers since 1st Nov 2017

- 14 new vulnerabilities reported
- 2 'Alerts'
- 2 'Critical' advisories
- Generally a bit behind on handling
  - Prioritized the more serious ones

FedCloud and contact lists

- Asked for lists for
  - VA Creators
  - VA Endorsers
  - VM Operators
- Can contact Endorsers (they are VO mangers) via the EGI BROADCAST tool
  - Only suitable for WHITE information
- Told a VA Creators list has been produced
  - Don't have the details yet, ability to send to it
- VM Operators
  - Not at present - VM Operator is a VO role

What is hardest? (As November)

- Proliferation of software, non-homogeneity both of software and configuration
- We don't know what software is running where, or how it is configured
- RAT cannot be experts in everything
- 'ALERT' used, but not the whole solution
- Also new services, which we know little about

Proliferation ideas (As November)

- Could have a list of ‘experts’ in certain areas.
- If someone chooses to deploy software on EGI, they need to volunteer to be an ‘expert’, take some responsibility?
- Should they be in the RAT?
- Or just who we contact?

AMBER Not just software bugs

- Software or services not complying with policy, not being as secure as we would like
- (amber removed)

- Not only simple ‘bug fix’ but on how services and software is designed

Different services (As November)

- People add things
- How to tackle
- Do they comply with policy?
  - I suggest see whether new services comply with policy
  - If not, flag to management
  - If does and still not happy, does policy need to change?
- Do we need a checklist for services?
  - Rather like the software checklist
- Do we need something like the Fed Cloud security questionnaire for other services?
  - Require those selecting services to fill in?

How to go forwards (broadly)

4 areas:--

1. Basic understanding of infrastructures and what services are in EOSC
2. Basic understanding of how the others do their security, including vulnerability handling
3. Security level that services should adhere to (policy, how services work)
   - Start with EGI and EUDAT services, see what their security is like
4. Software used and its proliferation (mainly SVG)
   - Again start with EGI and EUDAT.

What do we need?

- Good understanding of what is there, what are the components of EOSC.
  - We can't do security without knowing what we have
- We need a 'Map' of what is there.
  - What collaborating infrastructures are part of EOSC
  - Who is responsible
  - What services are on each infrastructure
  - Who are the contacts.
  - Not lots of details initially.
- Effectively a straw man diagram/list of what we have, and who to contact

Hierarchy of contacts –attached to 'Straw man'

- Contacts for the various infrastructures within EOSC
  - They should be able to tell us what services they provide
- Contacts for the services they provide
  - They should be able to answer questions on software, service etc. and who is responsible for configuration, software selection used
  - They should be 'software responsible' or delegate this
- Plus any contact for main areas of software development within EOSC

Straw Man Map important

- I think the straw man map and contacts are important, regardless of how we go forwards
  - However our long term co-operation is within EOSC
- It could be just a simple list of projects, services and who is responsible
  - Should not be difficult for management to provide
- Start asking management?
- Start with EGI and EUDAT, and establish what services are on there
  - Sometimes something is reported to us concerning a service we don't really know about

Other EOSC infrastructures and Security

- Should look at how other infrastructures do their security within EOSC
  - How do they handle vulnerabilities? Incidents?
  - Dave/Ian already plan to look at Policy
- With the Straw man, we should know who to contact
- Start with EGI and EUDAT
  - (This week)

Service Proliferation Contacts

- It is important to know what services are offered, and who the contact for each service is
- For each service, the Contact must take responsibility
  - Ensuring only good software is used
    - They may be or nominate software experts for software used
    - Where possible, standardise configuration
    - These look at the effect of vulnerabilities according to how they use the software, configuration etc.
  - Ensuring the service complies with the appropriate policies, works is a way security people think O.K.
    - Agree to abide by policies
  - Being able to answer questions, deal with problems

Service Proliferation – ideas

- We develop a questionnaire rather like the FedCloud site questionnaire
  - It includes references to the appropriate policies
  - Service contact fills this in
    - Someone looks at it?
- We develop a series of checklists/best practices/ references to policies
  - Service contact states they have read and understood
- Compulsory training – must have attended/certified

We need the contact details anyway in case of problems

Software proliferation – experts/contacts

- Software 'Experts' take responsibility
  - Check software against the 'Checklist'
    - May propose improvements to checklist
  - Look at configuration issues
    - Possibly provide wiki page describing how to configure securely
  - Look out for vulnerabilities
    - Report any announced and help with the investigation
  - Help if vulnerabilities are reported
- Some may join the RAT if they want to do wider work
  - Currently 33 members
- SVG still assesses the risk of vulnerabilities according to our criteria

Vulnerability handling across EOSC

- In the longer term, it would be good to have a common risk criteria, across infrastructures, even if different infrastructures do their handling separately
  - Possibly start with discussing vulnerabilities in software which is widely deployed, e.g. linux, and what the different infrastructures think
  - Similarly with OSG?
- Advisories for vulnerabilities in software in common use should be as simple as possible
  - And refer to public info

General vulnerability handling

- For vulnerabilities in e.g. operating systems
  - Keep them simple
  - Refer to public information where possible
- For vulnerabilities in software chosen by service providers, or written by them
  - Need more input from them
  - We can't do it all

Thank you for your attention.

Questions?

www.egi.eu