Software Vulnerability Handling in EGI

Dr Linda Cornwall, STFC, Rutherford Appleton Laboratory

Contents

- Purpose of EGI Software Vulnerability Group
- What do you do if you find a vulnerability?
- Why a vulnerability handling process?
- What is a vulnerability?
- Scope and types of Vulnerability
- Summarise issue handling process

Purpose of the EGI SVG

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

If you find a vulnerability

Report it to the EGI Software Vulnerability Group (SVG) by

e-mail to

report-vulnerability@egi.eu

What not to do

- You 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
- Please do not ignore it – better to have a report that turns out invalid than a serious vulnerability gets exploited

When you report a vulnerability

- You will receive acknowledgement
- You are invited to help and co-operate with investigation
  - Not mandatory – but would be good
- You will receive information, including the advisory if one is issued

Why a process?

- It was recognised in 2005 that vulnerability handling in the Grid environment was important
  - People were discussing vulnerabilities on open mailing lists
- Included the Grid Security Vulnerability Group (GSVG) in EGEE-II and EGEE-III
  - GSVG Issue handling process developed in 2006
  - Much of the EGI SVG issue handling process based on this and what was learnt
- No-one else handling vulnerabilities in much of the Grid middleware

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
  - Unauthorized user can gain access
  - Authorized user 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 attacker
  - Not usually treated as vulnerabilities
- General concerns
  - e.g. “these instructions are not clear”

Scope of SVG

- The main scope is to deal with software vulnerabilities in the EGI Unified Middleware Distribution (UMD)
  - – EGI has a Service Level agreement – with EMI(gLite, Unicore, ARC) and IGE
  - – This includes agreeing to e.g. response times
- Also handles other software (jointly with CSIRT) to provide consistent risk assessments.

Scope of SVG (2)

Software Source	S/W provider aware/announced vulnerability	S/W provider not clearly aware of vulnerability	Risk Assessment	Other comment
EGI UMD – e.g. **EMI/IGE software for which EGI has SLA**	Problem handled according to process in document by SVG		SVG	
Linux Operating system on which the EGI infrastructure is based	CSIRT/SVG investigates relevance to EGI	Inform software provider	SVG/CSIRT jointly	Usually CSIRT will contact provider if necessary
EPEL software **(Extra Packages for Linux Enterprise)**	CSIRT/SVG investigates relevance to EGI	Inform software provider	SVG/CSIRT jointly	SVG or CSIRT member will contact provider depending on knowledge
Other Software widely installed on the EGI Infrastructure	CSIRT/SVG investigates relevance to EGI	Inform software provider	SVG/CSIRT jointly	SVG or CSIRT member will contact provider depending on knowledge
Software not installed on the EGI infrastructure	Do nothing	Inform software provider	None	Only action is to forward information.

Issue handling process

- This is carried out by the SVG Risk Assessment Team (RAT)
  - The RAT has access to information on vulnerabilities reported
- 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 carries out a risk assessment
- Issue placed in one of 4 risk categories

  Critical, High, Moderate or Low
- Risk assessment carried out by the RAT because
  - mitigating or aggravating factors may exist in the Grid environment
  - Usually by consensus - the RAT usually agrees on the category
  - Say vote, but mostly agree on category

Issue handling (3)

- 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 (4)

- It is then up to the developers and release team to try and fix the problem by the Target Date or earlier
  - SVG will provide help and advice if appropriate
- Advisory issued when patch is available or on Target Date – whichever the sooner
  - Advisory refers to release notes, release notes refer to advisory
  - Advisories go to site-security-contacts and NGI-security-contacts

Critical Vulnerabilities

- New “EGI CSIRT Critical Vulnerability Operational procedure” which allows sites to be suspended if they fail to carry out updates to resolve or mitigate a critical vulnerability.
    - May apply for any type of vulnerability (operational, middleware, or operating system) assessed as critical
- So don’t ignore

More information

- Vulnerability Issue handling Process https://documents.egi.eu/public/ShowDocument?docid=717

  (currently under revision – no major changes)
- EGI SVG Wiki https://wiki.egi.eu/wiki/SVG:SVG
- EGI CSIRT Critical Vulnerability handling https://documents.egi.eu/secure/ShowDocument?docid=283

Questions?

- ??

Remember 1 thing

If you find a vulnerability:

Report it to

report-vulnerability@egi.eu