Software Vulnerabilities

HEPSYSMAN – July 2024 – Oxford

Linda Cornwall UKRI/STFC/RAL

I’m not a system manager

- Here mainly to take the opportunity to meet you and hear what you have to say.
- But I do run the EGI Software Vulnerability Group (SVG)
    - And send out most of the EGI SVG advisories

Purpose of the EGI Software Vulnerability Group (SVG)

To minimize the risk of security incidents due to software vulnerabilities.

GridPP sites get advisories as you know

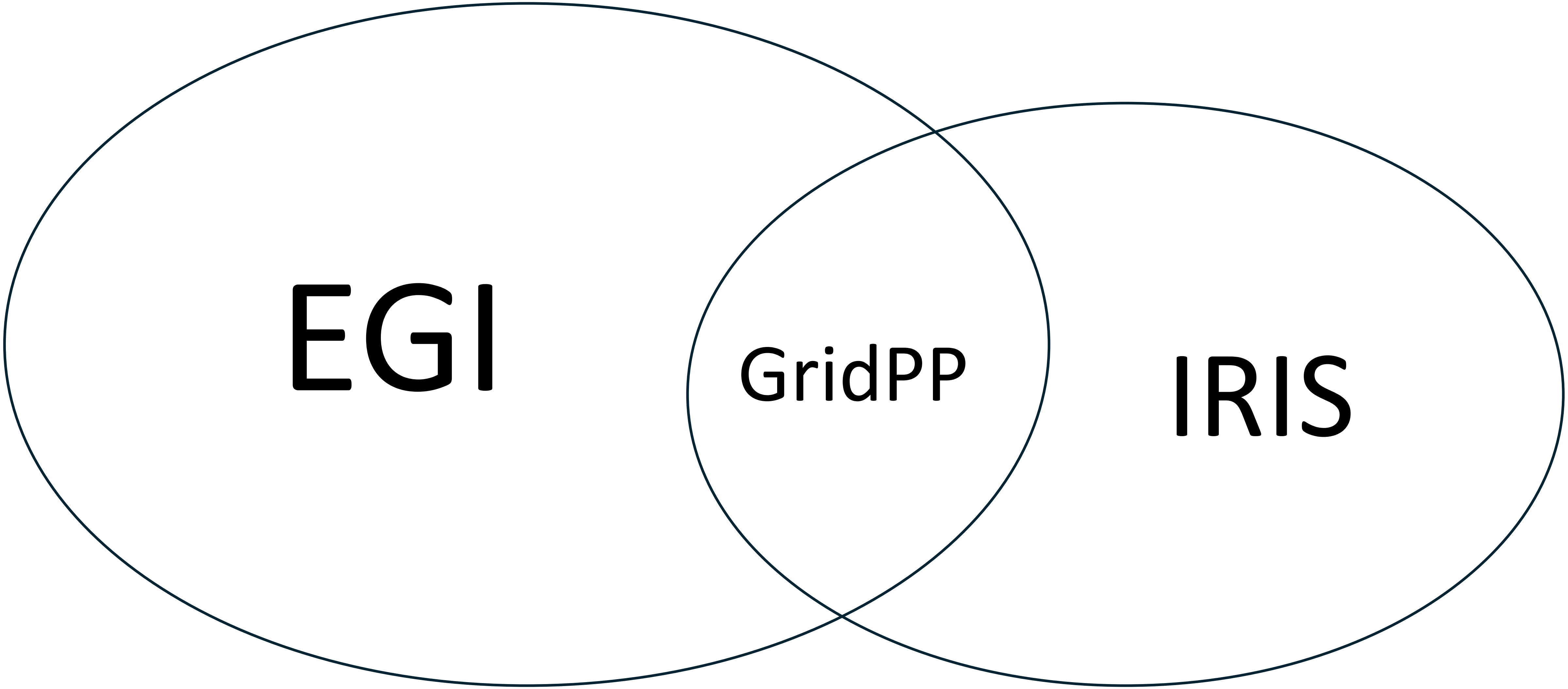
We think vulnerability handling is important

- It helps sites and data centres stay secure, – especially if there are less experienced staff
  - Helps share the load
- Sometimes due to the way software is used in a distributed infrastructure a vulnerability may pose a higher risk
- There may be other action, such as a configuration change which may be appropriate in a distributed environment
- Some software in use may be non-standard, e.g. written by those with which we collaborate with and vulnerabilities in this need to be sorted
  - This is getting less common in EGI
- User communities need to be confident that security is consistent in the distributed infrastructure they use.
- EGI also monitors sites for critical vulnerabilities, and contacts those exposing any defined as ‘Critical’

Current situation

- Within EGI, difficult to get more people involved in the EGI Software vulnerability Group
  - Especially for services other than Grid – e.g. Cloud
  - Less homogeneity – more proliferation of software/setup
- Forwarding advisories to others
  - OSG (who forward info to us)
  - 2 EUDAT people
  - 1 FNAL person
  - IRIS Vulnerabilities list
- Want to get more people involved, evolve to cope with greater variety of distributed infrastructures
  - Scope depends on participation
- Looking at planning for IRIS vulnerability group in the UK
  - To cover more than just GridPP
  - Working on defining how we do this

EGI, IRIS and GridPP



Questions?