EGI CSIRT

Mingchao Ma
EGI Security Officer
STFC - RAL UK

Introduction

- Overview EGI CSIRT activities since its establish
- Ongoing activities and roadmap revisited
- Challenges and Issues
- Discussion

EGI CSIRT Overview

- Officially formed on 1st May 2010
  - Built upon OSCT
- Smooth transit from EGEE era into EGI era
  - EGEE OSCT => EGI CSIRT
- EGI CSIRT now well established
  - Almost one year since beginning of EGI project
- Working closer with EGI SVG

CSIRT Overview

- Milestone MS405
  - https://documents.egi.eu/secure/ShowDocument?docid=47
- Produced two operational procedures, approved by EGI management and in operation now
  - https://wiki.egi.eu/wiki/Operational_Procedures
  - Security Incident Handling
  - EGI-CSIRT Critical Vulnerability Handling
- Continue improving internal procedures

CSIRT Overview

- Has issued 12 alerts
  - https://wiki.egi.eu/wiki/EGI_CSIRT:Alerts
  - of which, 3 are critical
    - 7-day deadline applied

- Handled 6 security incidents
  - All are traditional intrusion cases
  - No grid attack vector was known to be used, so far

Ongoing Activities

- IRTF
- Security Drills
- Security Monitoring
- Security Training and Dissemination

Roadmap Revisited

- Roadmap
  - https://documents.egi.eu/document/344

Challenges and Issues

- Increased number of sites and NGIs
- Limited manpower and resources
  - Probably all operational teams face the same challenge
- Need to smooth and improve both internal and external procedures
  - E.g. how to handle critical vulnerability which we can’t monitor

Discussions

- Risk assessment
  - How? Share your experience, please!
  - What to do with a site, a NGI or the EGI?
- Trusted Introducer
  - https://www.trusted-introducer.org/teams/teams-e.html#EGEE-OSCT
  - Need to update