EGI-CSIRT Critical Vulnerability Handling Procedure

Mingchao Ma, EGI CSIRT
STFC – UK

15th March 2011

Overview

- To handle time-critical security issue
- CSIRT decides which issue is CRITICAL based on risk assessment
- Ad-hoc procedure exist
- Based on the existing procedure and lessons learned from the day to day operation

The Procedure

- The goal is to improve overall EGI security instead of suspending a site!
- Who
  - Sites and NGI security officers
  - EGI CSIRT
  - EGI management - OMB
- Two scenarios
  - New identified vulnerability
  - Re-introduction of old problem

Procedure Summary

- A critical security issue identified
  - A head-up message from EGI CSIRT
  - to find a solution
- No solution is found in a reasonable timescale
- Solution available, send advisory with 7 calendar days deadline
  - to sites and NGI security officers
  - to EGI management: noc-managers mailing list
  - **7 days countdown starts**

Procedure Summary

- 3 days before the deadline
  - Ticketing outstanding sites as shown in our monitoring for actions
- 24 hours before deadline – final warning
  - To outstanding sites
  - To NOC managers for following up
- Throughout the process
  - CSIRT will help sites as much as possible
- At least 3 notification before suspension

Procedure Summary

- Re-introduction of old problem
  - Detect by EGI CSIRT monitoring tool
- 48 hours for site to solve the problem
  - Ticketing site when problem appears – 48 hours warning given
  - Contact sites again 24 hours before the deadline
    - NOC manager will also be informed

Site Suspension

- Site is warned
  - Final warning 24 hours before the suspension
  - OMB is informed as well
- Site suspension
  - Carry out by EGI CSIRT
- Senior management has the right to say NO
  - OMB and COO

Questions?