EGI-CSIRT – Operational Security

Sven Gabriel sveng@nikhef.nl, Nikhef, EGI-CSIRT

Activity Update

EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142

EGI-CSIRT OMB 29. Oct. 2015

Security Operations: Open Incidents

- Incident#9550:[EGI-20150925-01]: RootcompromiseatLCG-USTCandbitcoinmining
- 5 other sites affected (not all EGI)
- Close report expected for next OMB

EGI-CSIRT OMB 29. Oct. 2015

Security Operations: CRITICAL CVE handling

- open cases 3 cases still open (2 * CVE-2015-3245, 1 * CVE-2014-9322)
- new cases: 2 * CVE-2014-9322, 1 * CVE-2014-0160, 1 * CVE-2015-3245
- re-opened: 2 * CVE-2015-3245
- cases closed 5 (1 * CVE-2014-9322, 3 * CVE-2015-3245, 1 * CVE-2014-0160)
- Re-Certification: 1 Sites **in progress**.
- Re-Certification: 1 Sites **done**.

FedCloud Security

- Collaboration with FedCloud is improving.
- Currently checking communication channels to 6 FedCloud sites.
- Testing of Centralized User management with PERUN ready to test. Development done/coordinated by Boris Parak (NGI-CZ)

Procedure SEC03

- EGI-CSIRT Critical Vulnerability Operational Procedure
  https://wiki.egi.eu/wiki/SEC03
- Open questions about Security-Communication Channels?
- Approval status?