EGI-CSIRT Operational Security

Sven Gabriel, Vincent Brillault

Various updates

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

IRTF: Recent incidents

Recent incident: EGI-20180515-001

- Not EGI: Incident in a peer infrastructure
  - EGI CSIRT only involved in coordination
- Full compute site compromise:
  - First compromise outside the compute site
  - Compute compromised through lateral movement
  - Attacker (identified) goal: crypto-mining
- Two malicious IPs identified
  - No malicious activity on EGI sites, only scans
  - One compromised in another academic organisation

→ Good example of collaboration outside EGI!

Recent incident: EGI-20180618-01

- User-level compromise in an EGI site:
  - Site network ACLs down due to maintenance & error
  - Service accounts using weak password compromised
  - No evidence of escalation or lateral movement
  - Abused for network attack against SONY
- Compromised systems isolated & partially reinstalled
- No effect expected on the rest of EGI

Vulnerability update

Spectre v4: CVE-2018-3639

- Yet another CPU side attack
- Security Advisory sent on 2018-05-24 (High):
  - Kernel update required
  - Microcode update required, but not available
- Redhat & microcode update:
  - Position more clear: will release updates, but later
  - Still recommending to get update from manufacturer
  - As of now, no update for CVE-2018-3639
- Complex monitoring in Pakiti
  - Redhat continuously updated fix (PowerPC & AMD)
  - False positives in Pakiti: should now be whitelisted

$\rightarrow$ Sites still at risk until microcode released

Singularity: Another Overlay vulnerability

- Security Advisory sent on 2018-07-05 (Critical):
  - Not affecting RHEL/Centos/SL 6 (no Overlay support)
  - Can be mitigated by disabling Overlay feature
- Sites should update to 2.5.2
  - Packages now in EPEL (recommended distribution source)
- Discussions of formal security review in the US
  - Not before next major release (3.0): major rewrite

Security Service Challenge

Security Service Challenge

- Parts of the infra not finished, testing delayed
- Postponed to September

F2F Meeting

EGI CSIRT F2F Meeting Glasgow

- Excellent location, thanks to Univ Glasgow for hosting us
- https://indico.egi.eu/indico/event/4089/
- FedCloud: Updates on EGI infra and operations (Vulnerability handling).
- FedCloud: A security concept like security groups would be helpful
- Training: Debriefing of ISGC event, planning next trainings
- Monitoring, IRTF, SSC updates (day to day work)
- Collaboration EGI-CSIRT/EUDAT, no update

EGI CSIRT ReCertification

EGI CSIRT is recertified by Trusted Introducer (May 2018)