EGI-CSIRT – Operational Security

Activity Update

EGI-CSIRT

sveng@nikhef.nl, Nikhef, EGI-CSIRT

Activity Update / Overview

- Security Operations: Incidents / Alerts, Advisories
- Cloud Security
  - Evaluation of the questionnaires
  - Closer collaboration FedCloud EGI-CSIRT / Fedcloud F2F Jan 15 / Work packages defined
  - Participation Cloud Traceability workshop this Tuesday, February 10th, at CERN
- Collaboration EGI-CSIRT/WLCG: Pakiti and MW Readiness WG (No Update)
- Central Suspension (Monitoring, Emir?, Pending)

EGI-CSIRT OMB 26. Feb. 2015

Security Operations: Incidents / Alerts, Advisories

- Time period: 29. Jan – 26. Feb. 2015 / Alerts Advisories
  - 6 Vulnerability reports, 4 ’high’, 1 ’moderate’, 1 N/A
  - 5 Advisories
- No new incidents reported
- CRITICAL CVE handling
  - CVE-2014-9322: 13 Sites / 5 sites suspended
  - Re-Certification issues: ROD re-certified Site without contacting EGI-CSIRT, Language?
  - It should not be possible for RODs to re-certify Sites / No Control hook in this process.
  - CVE-2014-6271/6277 ShellShock 1 Site

Cloud Security

- Evaluation of the questionnaires finished https://wiki.egi.eu/csirt/index.php/Cloud_Resource_Providers_Questionnaires
- Not all policies accepted, issues with endorsed VM policy, Term processes is interpreted differently, different concepts in granting which access to the VMs.
- We can ”live” with that, though EGI-OPS might want to clarify some topics concerning Certification.

FedCloud Security

Cloud Security, EGI-CSIRT/FedCloud collaboration

- EGI-CSIRT / FedCloud security sessions at F2f in Jan 2015
- Goal: identified/agreed 3 work packages https://wiki.egi.eu/csirt/index.php/Operational_Security_FedCloud
- These are not yet part of the standing weekly agenda! Why?

FedCloud Security

Security Challenges in FedCloud Infrastructure I

- Communications Channel Challenges **DONE**, Boris
  - FedCloud Security Contact (Boris) subscribed to SSO EGI-CSIRT/IRTF
  - Docu: Howto run Communications Channel Challenges with RT-IR/GOC-DB
  - Sites contacted: 23 / Successful: 21 / Failed: 2
  - Failed sites (no response within 4 hours):
  - MK-04-FINKICLOUD – See https://rt.egi.eu/rt/Ticket/Display.html?id=8264
  - SZTAKI – See https://rt.egi.eu/rt/Ticket/Display.html?id=8267
  - All sites: See https://rt.egi.eu/guest/RTIR/Incident/ShowChildren.html?Queue=Investigations&id=8245

FedCloud Security

Security Challenges in FedCloud Infrastructure II

- Outline Challenge:
  - Start a VM / Fetch payload from external IP
  - extract/run payload, i.e. make connections to external hosts
  - Shutdown VM
- Tasks: The CRPs will get an IP together with a timestamp. Provide the following information:
  - what happened, when, how, and why, i.e.
  - DN who started the VM **traceability, sufficient logging info for an audit trail?** / if still running snapshot/suspend it
  - Suspicious network connections instantiated? to where?

FedCloud Security

Security Challenges in FedCloud Infrastructure III

- How: Is the DN or the VM compromised? Credential info leaked or Vulnerable software? **attack surface is multiple times larger then in Grid**
- VM identifier? (meta info), likelihood of more VMs affected by the same issue?
- Containment: Suspend DN (see WP User Management in IR) / Suspend VM-images (see WP VM Management in IR)

FedCloud Security

VM Management in Incident Response I

- Coordinator Boris
- Goal: Targeted Response / Minimize impact of incident response on user communities.
- Next steps: Finalize work plan

VM Management in Incident Response II

- Situation:
  - VM-Image found or reported to contain a Critical vulnerability.
  - Vulnerable VM-Image used by different users.
  - We get notified that this Vulnerability is actively exploited....
- Possible EGI-CSIRT responses (simplified):
  - do nothing until external parties complain, then shut down reported VM instances (cheapest solution, highest risk for EGI/CRPs reputation)
  - shut down all instances based on vulnerable VM-Image (cheap, will annoy users that rely on higher (then regular gird WN) availability of
  - leave "known good instances" running, shut down the rest.

FedCloud Security

User Management in Incident Response I

- Coordinator Boris
- Goal: Integrate argus based Central User Suspension in deployed cloud management systems
- Next steps: Finalize work plan
- Mischa Sallé provides consultancy on argus questions.
  - Open Questions/next steps:
  - What is needed to implement the described user suspension functionality in CMF (which?) services?
  - Who are the FedCloud tech experts to work on that?
- agreed Target date: PoC May Lisbon.