FedCloud Incident: EGI-20160509-01

What happened

- Incident reported by CESNET-MetaCloud 9th May 2016, other EGI-FedCloud Cloud sites are not able to detect incidents.
- Endorsed image got root compromised.
- Investigations revealed that a Malicious Contextualization script was downloaded from: **UPV-GRyCAP** https://goc.egi.eu/portal/index.php?Page_Type=Site&id=458
- Script configures VM to nfs export the home directory to the internet.
- This vulnerable configuration is actively exploited by various attackers by writing ssh keys to the exported home dir

FedCloud Incident: EGI-20160509-01

Problems in Incident handling

- Contextualization renders the Endorsement activity useless
- Site **UPV-GRyCAP** is not capable to support EGI-CSIRT in resolving the incident by providing basic logging data.
- Site **UPV-GRyCAP** claimed to have cleaned the Malicious script.
- This did obviously not work, another root compromised VM showing the same attack pattern was reported on 26th. May 2016.
- EGI-CSIRT requested the site to shutdown the service at least until sufficient logging is implemented.

FedCloud Incident: EGI-20160509-01

Next steps

- the attacker is actively trying to propagate and perform malicious activities from the breached machine.
- we potentially have large number of vulnerable instances.
- Site **UPV-GRyCAP** should shutdown the ”contextualisation” service untill:
  - logging is sufficiently implemented (as required by EGI policies)
  - the contextualization scripts are checked for vulnerabilities
- (Cloud) Sites should check for vulnerable configurations, EGI-CSIRT will support the sites.
- Evtl we have to request to blacklist **UPV-GRyCAP**