EGI-CSIRT Operational Security

Vincent Brillault, for the EGI IRTF

What happened since 2019-05-07

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

Recent Incidents

One single minor incident

- One (outdated) Jenkins server compromised
- Not part of any service, only with a site perimeter
- Properly handled by site and ngi

EGI services compromise Follow-up

- Incident in last April, reported to OMB in May
- Services were already *safe* in April
- Changes since last OMB:
  - Authentication services isolated & reinstalled
  - Mailman services isolated & reinstalled
  - Progress on other services
- Few services still being isolated & reinstalled

Vulnerabilities, Alerts & Advisories

Vulnerabilities, Alerts & Advisories I

- CVE-2019-11328: Singularity race condition
  - Only affecting systems with setuid = yes
- Intel Microarchitectural Data Sampling
- CVE-2018-1564: Docker race condition
- CVE-2019-1147{7,8,9}: Linux TCP SACK panic
- SQUID-2019:5: Frontier-Squid-4
  - Only affects frontier-squid-4.*, not 3.*

Security Service Challenge SSC-19.03

SSC-19.03 Update

- Draft reports compiled and sent to sites
- Few problems identified, e.g.:
  - Single ticket for two sites
  - Communication in another ticket
  - Site results mixed
- Hoping to send final version soon.

Any question?