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: None

- No security incident reported since last OMB

Vulnerability update

Intel Speculation Q3: L1TF

- Yet another CPU side attack (Q3)
- Security Advisory sent on 2018-09-04 (High):
  - Kernel update & reboot required
  - Hypervisors: Microcode required (& available)
  - Baremetal: microcode update recommended (SSBD)
- No known public exploit or exploitation in the wild
- Hypervisors & L1TF
  - HV with only 'trusted' VMs: VM kernel update enough
  - HV with any VMs (e.g. FedCloud): expensive mitigations needed (SMT off/CPU pinning/...)
  - Not possible to monitor from the VM...

→ No policy/hard requirement for FedCloud yet

Other Vulnerabilities

- CVE-2018-3110: sent on 2018-08-17 (Critical):
  - Only affects sites using Oracle Databases
- CVE-2018-10931: sent on 2018-08-17 (Critical):
  - Only affect site using cobbler, in certain deployments

Security Service Challenge

Security Service Challenge

- Parts of the infra not finished, testing delayed
- Postponed to a later date (not fixed yet)

Security Communication Challenge 2018

Communication Challenge 2018

- First EGI-wide challenge (past challenges: NGI)
- Workflow similar to Trusted-Introducer challenges
- Verification of GOC-DB security contacts:
  - Using RT-IR: signed email, ticket accessible
  - Asking to click on a single link
- EGI Operation helping to recover broken contacts

Communication Challenge 2018 Timeline

- Initial email sent on August 1st, 14:20-14:50
- Reminders sent on August 2nd, 15:11
- GGUS tickets open to NGI on August 6th
- 4 suspension warning sent on September 10th
- 1 site suspended on September 12th

Communication Challenge 2018 Results

- 23/272 clicks within 1 minute (8%)
- 101/272 clicks within 10 minutes (37%)
- 179/272 clicks within 1 hour (66%)
- 214/272 clicks within 4 hours (79%)
- 234/272 clicks within 1 day (86%)
- 252/272 clicks within 4 days (93%)
- 261/272 clicks within 7+ days (96%)
- 2 clicks at 39 days...
- 9 without direct clicks

Working-hour wise, these numbers are even better!

Communication Challenge 2018 Manual/special cases (11 GGUS+)

- 4 Ok after GGUS (spam folder, missed it, etc)
- 3 updated the mail contact
- 2 mails lost (unclear why/how)
- 2 with issues accessing RT
- 2 answer late in September (almost suspended)
- 2 sites closed by its NGI
- 2 EGI Core services to still be investigated
- 1 site to be decommissioned
- 1 site suspended by IRTF

Thanks for EGI Operation's help (Alessandro)!

Communication Challenge 2018 Conclusion

- Very good response time in general
  - Especially for the middle of the summer!
  - Example of 'worst' cases (summer, Christmas, ...)
- Benefits:
  - Keep contacts & access (e.g. RT) working/ready
  - Clean up outdated sites & contacts
- Cost:
  - Initial setup relatively expensive, but done
  - Several hours still required for manual cases
- Improvement considered for next time:
  Send mails in batch respecting sites' time zones

→ Expect another one next year!

Any other question?