EGI-CSIRT Operational Security

Sven Gabriel

Operational Security Update

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

Critical Vulnerabilities

- Various, no new CRITICAL Vulns

Incidents

EGI-20170825-01 Grid certificate exposure on Github

- Reported by Supervisor
- User exposed (pw protected credentials on Github)
- Certificate was revoked by CA immediately
- No traces of abuse in Accounting-DB, Panda

SSC

SSC FedCloud timeline

tentative time line (last OMB)

- week 26: Communication Challenge with potential sites, announcement.
- week 27: Tests/Announcement
- week 29: run
- week 30: evaluation/reporting

SSC FedCloud Report

- SSC- FedCloud was run from Jul 18 – 28. Juli (weeks 29,30)
- Requirement for participation: process the VM start/stop commands send from a rocci client to the OCCI endpoint at the RC.
- rocci wrapper script provided by EGI-Operations **Thanks!**
- only production IR tools used (goc-db, rt-ir, massticket)

Stage-1 Communication Challenge

Purpose of this stage is to make sure that the automated communication channels to the RC security teams are working as expected. For targeted communications in larger campaigns we use a tool developed within our team that, based on the RC names queries the GOC-DB for the RC and NGI security contact information and opens a ticket in RT-IR to the RCs, CCing the NGI security contact. The RCs were asked to acknowledge the message within 24 hours by replying to the mail/ticket.

Stage-1 Communication Challenge Results

Resource Center Name	Response Time
CYFRONET-CLOUD (NGI-PL)	<1h
CESGA (NGI-IBERGRID)	<3h
IN2P3-IRES (NGI-FRANCE)	<1h
INFN-PADOVA-STACK (NGI-IT)	<1h
INFN-CATANIA-STACK (NGI-IT)	<1h
RECAS-BARI (NGI-IT)	<3h
TR-FC1-ULAKBIM (NGI-TR)	<24h
IISAS-FEDCLOUD (NGI-SK)	<1h
CESNET-METACLOUD (NGI-CZ)	<1h
FZJ (NGI-DE)	<1h
BEGRID-BELNET (NGI-NL)	<2h
UPV-GRYCAP (NGI-IBERGRID)	<1h

Summary Stage-1 Communication Challenge

As a result we found that all RCs responded within the required time frame, the contact information in GOC-DB is up to date, and EGI CSIRTs communication tools are working as expected.

Stage-2 Compromised VM Challenge Participating Sites

- BEgrid-BELNET
- CESNET-MetaCloud
- CYFRONET-CLOUD
- IISAS-FedCloud
- IN2P3-IRES
- INFN-CATANIA-STACK
- INFN-PADOVA-STACK
- RECAS-BARI
- UPV-GRyCAP
- CESGA (NGI-IBERGRID)
- TR-FC1-ULAKBIM

Stage-2 Compromised VM Challenge

To be noted:

- FZJ dropped out. According to the test script we should have been able to start/stop VM, didn't work. Can't be debugged while running the SSC, sorry!
- IN2P3-IRES had a scheduled dt, nevertheless contributed!
- TR-FC1-ULAKBIM announced to be very short on manpower (holiday period) nevertheless contributed!

Stage-2 Compromised VM Challenge

To be noted: VMs at CESNET-MetaCloud were used as the development environment and gateway to control the VMs started at the RCs. The CESNET-MetaCloud security team kindly supported us with technical expertise on efficient FedCloud resource usage. As a result the were disqualified from that exercise, since they knew to much about the plans of the RedTeam.

Stage-2 Compromised VM Challenge

What we did / Actions to trigger RC IDSes

- Traceability: launched several VMs at the participating sites (2017-07-21 on or about 07:20:00) and let them idle for approx. 30 h before deleting them.
- 2017-07-25 04:36:15 Start SSC VMs
- 2017-07-25 14:24:59 Start DDOS / ”Crypto Mining like activity”

Stage-2 Compromised VM Challenge

SSC activity detected by:

- 2017-07-25T16:58:22+02:00 Incident reported by ReCaS-Bari, Unusual internet traffic at
- 2017-07-25T17:44:27+02:00 Incident acknowledged by EGI-CSIRT, asking for more detail
- 2017-07-25T18:58:20+02:00 Incident reported by CYFRONET-CLOUD ’ . . . instances generating large, possibly malicious . . . ” (detailed! report)
- 2017-07-25T20:01:08+02:00 Broadcast sent to Cloud-Sites-Security-Contacts.at.mailman.egi.eu

IRTF Broadcast sent Tue Jul 25 20:01:08 2017, timestamp 0 for IR, expected replies next 4 ”office hours”

Stage-2 Compromised VM Challenge

Replies by not participating sites, still checking there logs!

- 100%IT 25 Jul 2017 20:45:28
- FZJ 25 Jul 2017 20:50:00
- IFCA 26 Jul 2017 18:15:56 despite low on staff spotted the VM start/stop tries, dropped of the SSC since VMs did not got a puplic IP

Thanks for that, we will try to include your sites next time!

Stage-2 IR actions from sites
Prelim Results

Resource Center Name	ACK Time	Access to VMs suspended	DN suspended
CYFRONET-CLOUD (NGI-PL)	Reporting RC	0 h	
RECAS-BARI (NGI-IT)	Reporting RC	1d +	
IN2P3-IRES (NGI-FRANCE)	25 Jul 2017 22:20:04	SDT	
IISAS-FEDCLOUD (NGI-SK)	25 Jul 2017 22:35:20	2 h	
BEGRID-BELNET (NGI-NL)	<4h	3 h	
INFN-CATANIA-STACK (NGI-IT)	2d +	8h +	
TR-FC1-ULAKBIM (NGI-TR)	2d +	No ssh	
UPV-GRYCAP (NGI-IBERGRID)	2d +	12h +	
CESGA (NGI-IBERGRID)	2d +	NO IR	NO IR

Stage-2 IR actions from sites

CESNET-METACLOUD (NGI-CZ) were providing SSC infrastructure, were asked to not intervene.
CESGA (NGI-IBERGRID) Was answering to a ticket opened for UPV, found VMs from the testing phase before SSC
INFN-PADOVA-STACK (NGI-IT) In scheduled downtime, upgrading.

Summary I

- Activity was spotted!
- Many useful ”after hours” contributions!
- RC Sec teams worked on the topic despite seasonable little available manpower.
- Nice Forensics from CYFRONET!
- User/VM management to be improved, reassessed.
- Central IR tools not tested here, lack of implementation, should be revisited.
- Communication issues/coordination issues in one region, to be checked.
- This was fun!

Summary

This is the first SSC addressing the EGI FedCloud RCs. Although only 50% of the FedCloud RCs were available for the challenge, the results nevertheless provide an initial assessment of the EGI FedCloud's readiness to respond to an incident and give directions for a possible RC certification challenge and a future SSC addressing more FedCloud RCs, reassessment of issues found

Summary Missing/Unclear Results

- User Management! No Central tools used, Results of user managenment at sites unclear
- Differentiated assessment of different ”Mechanisms” (VO,CA,Central Suspension) to be redone
- Central Suspension does **not** work in FedCloud
- Needs to be redone!

Summary Next steps

- Detailed report to the RCs, OMB.
- Present/Discuss results at next conference.Which?

Procedure Update

SEC05: new proposal

HTC Clarify communications between RC, OC & CSIRT

HTC New steps:

- Make sure that the site is up to date with regard to security patches.
- Check on pakiti that the report was sent and that no critical vulnerability was found.

Cloud Clarify communication paths

EGI-CSIRT Report/OutReach

EGI-CSIRT Report/OutReach

- WebPage https://csirt.egi.eu
- Purpose: presentation of EGI CSIRT activities and publication of reports, presentations etc. The policies, tutorials, advisories etc will remain on the wiki.
- EGI CSIRT activities report 2017: Keeping the EGI Secure https://www.egi.eu/wp-content/uploads/2017/07/EGI-CSIRT-report-July-2017.pdf

THANKS: Barbara, Sophie, Ian (Webpage), IRTF + Sara for the report