#13

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Tuesday, January 24, 2017 11:36:22 PM
Last Modified: Tuesday, January 24, 2017 11:45:07 PM
Time Spent: 00:08:45
IP Address: 217.42.113.125

PAGE 1: Report on performance of the service

Q1: Service — Security coordination and security tools

Q2: The reporting person:

Name	David Kelsey (STFC)
E-mail	david.kelsey@stfc.ac.uk

Q3: EFFORT(Please provide effort (PM) spent by each partner (separately) during the whole reporting period.)

During these 4 months we all spent at least according to the allocations. In addition many partners provided additional (funded or unfunded) effort not reported here.
CERN 1.67 PM
CESNET 1.33 PM
GRNET 0.80 PM
Nikhef 2.20 PM
STFC 2.67 PM

TOTAL 8.67 PM

Q4: GENERAL OVERVIEW OF ACTIVITY IN THE PERIOD(Short prose overview of what happened in the period. Things went well? There were problems but they were addressed? There were significant problems that persist and must be dealt with?)

The Security Coordination and Security Tools functions performed well during another busy period for operational security. Coordination activities were carried out as expected in collaboration with EGI-Engage including regular weekly/monthly/face to face meetings and active participation in events. Reports were presented at the monthly EGI OMB meetings. A CSIRT F2F meeting was held in Abingdon (8/9 Sep) and planning took place for the CSIRT F2F meeting in Prague (Jan 2017). An SPG F2F meeting was held in Nikhef (2/3 Nov). Plans for the EINFRA-12 proposal were prepared and submitted (Sep and Nov).

EGI was represented and members of the team played leading roles at many different meetings, including TF-CSIRT in Zurich (20-21 Sep), SIG-ISM in Trondheim (12/13 Sep), WISE/DI4R in Krakow (27-30 Sep), GEANT/EGI/EUDAT/SURFnet security meeting in Cambridge (8/9 Dec).

Coordination of IRTF, which:
- Handled several security incidents: EGI-20161013-01, EGI-20161124-01, EGI-20161214-01 and EGI-20161229-01 (resolved later in January). 3 out of 4 of these incidents came from the Federated Cloud.
- Handled critical vulnerabilities. There were two major campaigns chasing patching of the infrastructure to fix these.

One security incident [EGI-20161214-01] started off as one EGI compromised server running malware. Detailed forensic analysis found that this was a more wide-spread attack involving many more systems. The EGI CSIRT prepared a detailed report on the VENOM Linux Rootkit (to be released to the security communities in January).

The number of RT-IR tickets created in the period was 273. A further 312 old RT-IR tickets were modified. Four GGUS tickets were handled during the period, well within the SLA-defined time limits.

This was a busy time for the SVG Issue handling with 11 new issues were reported during these 4 months. This includes 1 assessed as 'Critical' risk and 3 'High' risk. Seven advisories were issued on the public wiki. Minor updates were made to the Advisory template, including context section describing that the risk is the opinion of SVG in the context of the EGI deployment.

SPG, in collaboration with EGI-Engage, at its F2F meeting in November produced several updated policy documents, including a new top-level overall Security Policy. These are now going through the formal approval procedure.

The trust anchor distribution was updated three times. Improvements were made to resolve issues with Debian packaging tools. Preparation continues for the inclusion of the on-line "IOTA" CA. Chaired EUGridPMA/IGTF All Hands meeting at CERN (19-21 Sep). EGI was represented in the IGTF F2F meetings in the Americas (24/25 Oct).

For SECMON:
• 02 Sep 2016: Call for SECMON
• 15 Sep 2016: Solved communication issues between secmon and Pakiti (ggus #123744)
• 30 Sep 2016: Removed probe eu.egi.sec.WN-check_EGI-SVG-2013-5890-ops
• 24 Oct 2016: Added probes for CVE-2016-5195, EGI-SVG-2016-5195 (ggus #124719)
• 22 Nov 2016: Updated probes for CVE-2016-5195, EGI-SVG-2016-5195

Evaluation of results produced by security probes and issues detected. Supporting on-duty members of EGI-CSIRT with monitoring needs and addressing certification requests.

Participated in WISE Steering committee meetings, co-chaired WISE workshop in Krakow (Sep), prepared for WISE workshop in Nikhef (March 2017).

Q5: ISSUES ARISING IN THE PERIOD(Explain issues, such as OLA violations or other problems in performance. Also consider other events that may not lead to violations, such as planned downtime, or problems in services there is a dependency on.)

The security incident in November has shown again that the EGI FedCloud, especially for sites that do not restrict incoming network activity by default, can lead to basic security issues, that we would not expect on well-maintained modern sites... (for example world-writable NFS exports, default basic passwords).

Emergency suspension is not yet deployed in the Federated Cloud (requires developments, especially for Openstack sites). This is now part of mid-term plan of the Federated Cloud, but in the meantime no progress can be made.

There are no known issues or SLA violations for operational security coordination or trust anchor management.

SECMON is still running on Centos5 and using the old SAM framework as there are is no effort available for changing the platform.

Q6: MITIGATION ACTIONS PLANNED (Explain action planned to mitigate issues in this period.)

The FedCloud team is working on emergency suspension.

Q7: FORESEEN ACTIVITIES AND CHANGES (Note upcoming activities or changes impacting the service and OLA that are the subject of this report. For instance planned ending or renegotiation of the agreement or planned major upgrades to the service, new activities.)

Most operational security activities will continue as before. IRTF changes will depend on incidents and policy discussions. However, if the FedCloud expands (more user and more providers), we have to prepare ourselves to handle more incidents.

Still need to progress contacts relevant to the EGI Federated cloud, as we still do not have means of easily contacting VM endorsers or VM operators. Look at whether there needs to be other adaptations to SVG issue handling process for FedCloud and other changing technology.
Re-visit and clearly define scope of SVG, concerning changing technology.

SPG will produce revised policies on VO operations and management, in collaboration with EGI-Engage. For the trust anchor distribution, no changes to the operational service are foreseen. The integration of the IOTA "RCauth.eu" CA in the EGI trust anchor framework may lead to an increase in questions regarding the trust model.

We will hold a CSIRT F2F meeting in Prague in January. Participation and leadership of WISE and IGTF activities including two PMA meetings will continue. SCIv2 will be completed and presented at TNC2017 in Linz.

Many of the team will speak and/or chair sessions at the ISGC2017 conference in Taipei and the WISE workshop at Nikhef (both in March). We will participate in the EGI conference in Catania (May)

SECMON – Operation of the service.

Finalise the security parts of the EINFRA-12 proposal.