OSG Security AC Meeting 19July2017

Jeny Teheran presenting for Susan Sons

July 19, 2017

Activities, Recent and Upcoming

- Completed deployment of Yubikeys for CVFMS Master key
- Zalak currently working on refactoring our process and scripts for producing certificate bundles to remove dependency on Globus Toolkit. A rough working version is on Github[1].
- Susan to attend NSF Summit on behalf of OSG, August 15-17
- Susan will be at the OSG planning meeting next week, July 25-26.
- Jeny worked with Jim Basney to update Grid Admin (RA) form to reflect that we're no longer using Digicert.
- Dave is working on a python plug-in to track Singularity jobs via Condor...this is in testing stages.
- Susan has begun work on next year's Security Team goals. Suggestions/requests/wishes-for-ponies welcome.

[1] https://github.com/opensciencegrid/secteam-tools

Vulnerabilities since last AC Meeting report on 17 June

- Security advisory from EGI SVG regarding vulnerabilities in Qemu and Xen (rated as High)[2]. OSG security team did not send an announcement this time because it was highly unlikely to have OSG jobs affected due to these vulnerabilities.
- CILogon (Jim B.) reported that some OSG certificates were in violation of the CILogon OSG CA CP/CPS naming policy. These certificates were intended to be used as service certificates, but were requested as user certificates and the RAs did not check the requests properly. OSG security team has updated the request forms for GAs and RAs. Training material for VO security contacts has been updated as well.
- Security announcement regarding the Stack Clash vulnerability[3]. This vulnerability allows an attacker to corrupt the memory and do privilege escalation, gaining root access, for example. The OSG community was notified and OSG Security Team requested to apply the packages security updates from the vendors.

[2] https://ticket.opensciencegrid.org/33993

[3] https://ticket.opensciencegrid.org/34210

- Updated announcement regarding VOMS-admin package which was published JuneâĂŹs scheduled OSG Software stack release. The announcement also reminded people that VOMS-admin package is being dropped from OSG 3.4 and retired definitely in June 2018.

Security Goals: Year5 Update

1. Fix weakness in traceability mechanism for certificate-free jobs: **COMPLETE**
2. Store CVMFS master key on secure hardware token: **COMPLETE**
3. Complete a review of the security program: **COMPLETE**[4]
4. Establish a static analysis workflow and evaluate for adoption throughout OSG: **IN PROGRESS**[5]
5. Create a secure and automated mechanism to generate host certificates: **IN PROGRESS**[6]
6. Maintain operational security: **IN PROGRESS**[7]
7. Complete OSG Cybersecurity Risk Assessment: **COMPLETE**

[4] Will report at planning retreat.

[5] Proof-of-concept workflow is in place, and some results have been produced. Feedback from software maintainers has been that this is a hard-to-prioritize firehose of data, Security Team welcomes more specific recommendations as we put together some requests for SWAMP.

[6] The move of the CVMFS master key to hardware tokens for secure, constant availability was the first step in this process.

[7] Ongoing. See section above on vulnerabilities since last AC meeting report.