OSG Security AC Meeting 13September2017

Susan Sons

September 13, 2017

Activities, Recent and Upcoming

- We have confirmed that RHEL7.4 enables Singularity to run without setuid-root, using newly available kernel feature.
  - Great reduction in attack surface, increase in compartmentation
  - New kernel feature is at this point is a technology preview, not enabled by default, which requires setting a boot parameter.
  - Dave Dykstra has added details in the OSG Singularity installation documentation.
  - We have installed unprivileged Singularity in CVMFS.
  - GlideinWMS will try running Singularity from CVMFS first before /usr/bin.
- Jeny providing certificate request refresher course in four sessions throughout September to help cut down on malformed requests.
- More Apache Struts vulnerabilities are expected over the next year or two; Struts is only present in voms-admin which is already slated for EOL within OSG during 2018.

Vulnerabilities since last AC Meeting report on 17 June

- The dCache team has reported that an old vulnerability from 2015 concerning the "gridftp door", and the "kerberos ftp door" of dCache has been re-introduced. Due to this vulnerability, the dCache server accepts unencrypted commands. This vulnerability allows a MITM (man-in-the-middle) attacker to execute unencrypted commands on behalf of an authenticated user. The attacker is restricted to execute only the commands the authenticated user is authorized to.
  - Announcement sent back in 2015: https://ticket.opensciencegrid.org/26855
  - Announcement sent in August 2017: https://ticket.opensciencegrid.org/34800
- The Apache Struts Group released Struts 2.5.13 on September 5th, 2017. This release fixes 3 security vulnerabilities, including a possible remote code execution attack when using the Struts REST plugin.

Security Goals: Year6 Update

1. Ongoing Responsibilities: Assist other teams with security expertise as requested, lead IR and vulnerability response. **ONGOING**
2. Ensure the creation and maintenance of an up-to-date asset inventory for OSG.[1] **BEGINS OCT2017**
3. Produce an OSG Cybersecurity Strategic Plan **IN PROGRESS**[2]
4. Reduce OSG's dependence on user x.509 certificates. **IN PROGRESS**[3]
5. Perform OSG Annual Risk Assessment **BEGINS OCT2017**[4]
6. Continue last year's effort to identify and automate machine-repeatable security processes. **IN PROGRESS**

[1] Working in close concert with ops to avoid duplication of effort, build on existing data collection.

[2] Draft expected to circulate late Oct2017.

[3] This is to be accomplished through supporting Ops' Marina Krenz work on SSO for OSG web properties, and working with European grid communities on trust for non-user-certificate based auth plans in the far future.

[4] Area Coordinators can expect to be contacted in Oct-Nov 2017.