OSG Area Coordinators Meeting Security Team Report

Kevin Hill

08/14/2013

Key Initiatives

- Traceability
  - Traceability findings presented to Fermilab CS Board.
  - Committee was to be formed to draft changes to security policy changes to allow job submission without end user x.509 certificates.
  - Have not heard back on progress.
  - This is on the schedule for this Friday's CS Board meeting.

Key Initiatives

- CILogon Basic CA adoption
  - Fermilab is now accepting CI Logon Basic CA certificates issued for individuals at
    - University of Illinois
    - University of Wisconsin
    - University of Chicago
    - Indiana University.
  - Ran test to see how many CEs have CI Logon Basic CA cert installed.
    - Found 25/75 CEs at 4-5 unique sites have it installed currently.

Operational Security

- There was an issue with a certificate in the OSG CA cert bundle expiring before the new version with a refreshed certificate was available.
  - This was a case of the igtf lead time vs. the software release freeze time not quite matching up.
  - In response we've set up a system to alert us if any CA cert is going to expire in the next 60 days.
- New CA cert bundle released at end of June. Next expected at end of August.
- Investigated possibility of ca cert bundles cleaning up orphan certificates on removal/upgrades.
  - This functionality is coming in a future release of fetch-crl, so won't be added to the ca bundle rpms.

Operational Security

- Recent security advisories
  - OSG-SEC-2013-06-19 Security vulnerability in Puppet allowed remote code execution.
  - OSG-SEC-2013-07-26 Security vulnerability in PHP allowed remote code execution.
  - OSG-SEC-2013-08-13 Security vulnerability in CVMFS allowed local privilege escalation.

Top Issues / Concerns

- Mine out until October, Kevin Hill acting Security Officer.
- Extending CILogon adoption:
  - Chicken/Egg issue in VOs need to register users with the certs as well as sites accepting them.
  - Now that we can check which sites are ready to accept CI Logon Basic certs, we can approach VOs with numbers on how many sites will accept.

Accomplishments

- Run security-related meetings with 1 new OSG VO. 1 more coming up.
- Security Controls assessment mostly complete. Still waiting for a few straggler service owners to complete surveys.

	WBS Ongoing Activities	
1	Incident response and vulnerability assessment	Minimizing the end-end response time to an incident, 1 day for a severe incident, 1 week for a moderate incident, and 1 month for a low-risk incient.
2	Troubleshooting; processing security tickets including user requests, change requests from stakeholders, technical problems	Goal is to acknowledge tickets within one day of receipt.
3	Maintaining security scripts (vdt-update-certs, vdt-ca-manage, cert-scripts, etc)	Maintain and provide bug fixes according to the severity of bugs. For urgent problems, provide an update in one week; For moderate severity, provide an update in a month; For low risk problems, provide an update in 6 months.
4	XSEDE Operational Security Interface	Meet weekly
5	Supporting OSG RA in processing certificate requests	Each certificate request is resolved within one week; requests for GridAdmin and RA Agents are served within 3 days.
6	Preparing CA releases (IGTF), modifying OSG software as the changes in releases require	CA release for every two months
7	Security Policy work with IGTF, TAGPMA, JSPG and EGI	Meet with IGTF and TAGPMA twice a year. Attend JSPG and EGI meteings remotely and face-face once a year. Track security policy changes and report to OSG management.
8	Security Test and Controls	Execute all the controls included in the Security Plan and prepare a summary analysis.
9	Incident Drills and Training	Drill Tier3 sites
10	Weekly Security Team Meeting to review work items	Coordinate weekly work it ems.
11	Weekly reporting to OSG-Production	Report important items that will affect production; incidents, vulnerabilities, changes to PKI infrastructure