OSG Security AC Meeting 07June2017

Susan Sons

June 7, 2017

Activities, Recent and Upcoming

- Pursuing Yubikey deployment for CVFMS Master key
- Susan to attend NSF Summit on behalf of OSG, August 15-17
- Changed SecTeam meeting agenda/notes to Google Doc with good results
- Jeny is working 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.
- Susan has begun work on next year's Security Team goals. Suggestions/requests/wishes-for-ponies welcome.

Vulnerabilities since last AC Meeting report

- Apache Struts vulnerabilities affecting VOMS-admin package. Issue reported initially by EGI SVG. They produce a quick patch and send instructions to their sites promptly.[1] An announcement was sent to the OSG Community.[2]
- VOMS-admin package with vulnerabilities fixed scheduled for release on June 13th.
- Issue concerning credential caching on HT-condor CE which leads to delayed effect on GUMS banning.[3]
- Linux Kernel local privilege escalation vulnerability[4] Issue was addressed quickly at GOC.[5]
- Vulnerability in NSS reported in CVE-2017-5461[6]. Potential DoS and arbitrary code execution.
  An announcement was sent to OSG community.[7]
- Announcement to OSG community[8] regarding TLS/SSL filtering issues triggered by well-known IPSs as TippingPoint? and Fortios. A couple of OSG sites have reported having handshake timeouts in file transfers due to network blocking triggered by these IPSs. According to the reports received from the sites, a new

[1] `https://ticket.opensciencegrid.org/33099`

[2] `https://ticket.opensciencegrid.org/33418`

[3] `https://ticket.opensciencegrid.org/33278`

[4] `https://access.redhat.com/security/vulnerabilities/CVE-2017-2636?`

[5] `https://ticket.opensciencegrid.org/33514`

[6] `https://access.redhat.com/security/cve/cve-2017-5461`

[7] `https://ticket.opensciencegrid.org/33569`

[8] `https://ticket.opensciencegrid.org/33724`

filter targeting a vulnerability the GnuTLS library, is flagging all TLS connections that involve a grid proxy (RFC3820). [9]

- Security advisory from EGI SVG regarding vulnerabilities[10] in Qemu and Xen (rated as High): GOC machines were already patched in the scheduled maintenance. HTCondor can use Qemu/Xen for its VM universe. However, it is highly unlikely that HTCondor would be affected by the vulnerabilities in Qemu or Xen which are in the VNC interface. By default, the HTCondor job does not create a VNC interface. The risk of having these vulnerabilities exploited in the grid nodes is extremely low.

Security Goals: Year5 Update

1. Fix weakness in traceability mechanism for certificate-free jobs: **COMPLETE**
2. Store CVMFS master key on secure hardware token: **IN PROGRESS**[11]
3. Complete a review of the security program: **COMPLETE**[12]
4. Establish a static analysis workflow and evaluate for adoption throughout OSG: **IN PROGRESS**[13]
5. Create a secure and automated mechanism to generate host certificates: **IN PROGRESS**[14]
6. Maintain operational security: **IN PROGRESS**[15]
7. Complete OSG Cybersecurity Risk Assessment: **COMPLETE**

[9] https://ticket.opensciencegrid.org/33610

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

[11] Ready for production: meeting next week with Scott Tiege to address deployment concerns.

[12] Will report at planning retreat.

[13] Proof-of-concept workflow is in place, and some results have been produced. We are waiting on feedback from software maintainers as to how helpful this is and what they would like to see done differently.

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

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