SOFTWARE SECURITY WORKING TEAM
PROGRESS & NEXT STEPS

ESGF F2F Workshop,
Washington, DC, December 2016

<< George Rumney - Working Team Lead >>

2016 Progress & Accomplishments

- Software security plan was approved by the XC (published April 2016)
- Software release procedures were established, with emphasis on scanning - code and live services
- Source code scans, Live web scans, & Configuration reviews were conducted
- JAR file “scanner” was created but is manually intensive (many false positives)
- Version 2.3 was released following scans and reviews and disposition of findings
- Risk-based process, the intention of which is to avoid issuing a release with elevated risk (to avoid a repeat of something similar to the June 2015 “Apache Struts” incident)
- We are better able to detect such issues in advance, but risks remain (e.g., Solr), both in the Code base and in the procedures
- Membership in SSWT was established (esgf-sswt@llnl.gov)

2016 Missed Milestones (if any)

Software Security Plan requirements:

- ESGF Risk Executive not yet identified (ref: NIST SP 800-39)
- Software Development Team and Security Team not yet integrated to coordinate ESGF software design
- Manifest of software remains incomplete for third-party software
- Security is not yet fully a part of the software engineering process.

Shortfalls

- Installation is still cumbersome and fragile (monolithic and prone to failure)
- The large ESG software footprint is challenging efforts for risk reduction
- Included software (e.g. Tomcat…) makes patching challenging
- The lack of a modular build process (modularity would increase maintainability and enhance local site control)

2017 Roadmap

SSWT plans to:

- Support integration of Software Development Team with Software Security Team efforts (requirements baseline, alternatives analysis, requirements for future releases, etc.)
- Maintain and enhance the software manifest of installed components
- Implement Federal requirements: SSL & IPV6
- Implement SELinux (enforcing mode is being required by NASA)
- Support establishment of the ESGF Risk Executive
- Perform vulnerability determination and risk assessment for next release
- Support software engineering efforts to reduce risk, increase maintainability
- Define best practices for site installations (e.g., local firewall rules)

Additional Resources Needed (if any)

- SSWT supports the allocation of resources for the re-design and re-implementation of the install process;
- Other sites contribution (e.g., JPL, NOAA) will be required to aid scanning efforts, both source code base and live web scans;
- ESGF Risk Executive reviews (most resources will come from the ESGF-SSWT), as needed;
- SSWT team members' contribution to define best practices, as needed.
- Licenses for source code scanning ($$$).

Collaborations Needed (if any)

- SSWT collaboration with other ESGF working teams
  - Software Development Team
  - Risk Executive
  - Executive Committee
- Collaboration with ESGF sites (to perform scans, risk assessments, best practices)
- Collaboration with outside entities
  - None