OSG Service Container Security Policy

Version 1.0

Last updated on 12/1/2019

Author: Mike Stanfield

Information Security Officer: Mike Stanfield

1. Reason for Policy

This policy is intended to describe how the Open Science Grid (OSG) ensures service containers deployed by OSG and sites are built and maintained in a secure manner. By defining the Security Team's expectations regarding container configuration, we ensure that all relevant teams understand the necessary requirements and precautions laid out in Section 2 below.

Since the service container images developed by the OSG Software Team are often deployed at the network edge and are accessible from the Internet, it is important that we have a standardized way of building and updating these images in order to minimize the risk to these edge services.

This policy defines basic security requirements for new and existing service containers, a process for updating container images in a timely manner, and the exception process.

2. Policy Statement

- Service container images must be based on the most up to date, OSG-supported upstream OS container images, and should be rebuilt weekly.
- The base OS container image must be updated with the latest security updates from the upstream providers.
- Service container images intended for production use should use the "latest released" version of the service software when possible.

Additionally, a process must exist to allow the Software Team to manually rebuild a container image should immediate, emergency rebuild become necessary in the course of a declared security incident.

2.1. Exceptions

Exceptions to this policy must be documented and reviewed by the Security Team per Section 3.2 of the OSG Master Information Security Policy & Procedures document..

3. Adhering to this Policy

New container images must be validated by the Software Team to ensure compliance with the requirements laid out in Section 2, with the Security Team providing guidance when necessary. Container images should also be checked for compliance with the requirements in Section 2 by automated tools prior to being pushed to public repositories and upon update. Additionally, automated tools should be used to ensure that container images do not contain any known

vulnerabilities. Container images that fail automated validation should be triaged, and if necessary an exception should be requested as laid out in Section 2.1 of this policy document.

An ideal automated scanning solution will ensure, with each change registered in the continuous integration system, that:

- All upstream packages in each base image are at the best-available security patch level.
- Common security-related misconfigurations and past OSG misconfigurations are not present.

However, we acknowledge that it will take time to get such a system in place, and in the meantime manual review by the Software Team is considered acceptable.

The Security Team recommends that any teams running OSG service containers restart their containers weekly to ensure they are running updated images. Additionally, teams running service containers should consider peristing their application logs to a seperate volume or sending them to a remote log server.