

Preventing security incidents in the EOSC-hub era - by evolving Software Vulnerability Handling

Wednesday, 10 October 2018 16:50 (5 minutes)

The EGI Software Vulnerability Group (SVG) has been handling software vulnerabilities in order to help prevent security incidents in the EGI infrastructure and its predecessor, the EGEE series of projects, for more than a decade. While the procedure has evolved somewhat it has remained focussed on the fairly well defined Grid and later cloud technologies having a fairly standard configuration, with vulnerabilities mostly investigated and risk assessed by the SVG 'Risk Assessment Team' or 'RAT'.

During the last year it has become clear that major changes are needed to the way the SVG handles software vulnerabilities due to the proliferation of software and technology, other collaborating infrastructures, lack of homogeneity and above all the services in the EOSC-hub service catalogue. The current 'RAT' cannot be experts in all the various types of software and services, and how software is configured and deployed. Those selecting software or deploying services will need to take responsibility for investigating vulnerabilities in software used to enable their services and the risk to those services.

This talk will describe how we plan to evolve the SVG issue handling procedure so that those who select and deploy software and services have a greater role in vulnerability handling, while aiming for a consistent risk assessment so that the most serious vulnerabilities get priority in their resolution. This will include plans for smooth communication with relevant parties such as experts in specific software, infrastructure providers, as well as those providing specific services in the EOSC-hub catalogue which depend on specific pieces of software. It will also inform service providers what they should do to help SVG to help them ensure that their services are as free from vulnerabilities as possible, to minimize the risk of security incidents due to software vulnerabilities concerning their services.

Type of abstract

Lightning Talk

Summary

This briefly describes plans for evolution of software vulnerability handling in the EOSC-hub era, in order to take account of the proliferation of software and services in the EOSC-hub catalogue.

Primary author: CORNWALL, Linda (STFC)

Presenter: CORNWALL, Linda (STFC)

Session Classification: Lightning Talks

Track Classification: Lightning Talks