Contribution ID: **11** Type: **Presentations**

EGI Software Vulnerability Handling after EMI and IGE

Thursday, 11 April 2013 14:00 (45 minutes)

Impact

As far as we are aware, no security incidents have occurred due to vulnerabilities in Grid Middleware.
It is important that the vulnerability issue handling continues, in order to keep it this way.

Summary

The goal of the EGI Software Vulnerability Group (SVG) is "to eliminate existing software vulnerabilities from the deployed infrastructure and prevent the introduction of new ones, thus reducing the likelihood of security incidents". The largest activity of the SVG is to handle vulnerabilities reported according to an agreed procedure and clearly defined process. The emphasis is on software vulnerabilities in Grid Middleware which are not handled elsewhere, and the majority of the work concerns European Middleware Initiative (EMI) software, and some concerns Initiative for Globus in Europe (IGE) software. The need for this activity will continue after the end of EMI and IGE. This talk will describe what is likely to remain the same and what is likely to change after the end of the EMI and IGE projects.

Description

A vulnerability may be defined as a weakness allowing a principal (such as a user) to gain access to or influence a system beyond their intended rights. An incident is where a vulnerability has been exploited and unauthorized access or activity has taken place.
The EGI Software Vulnerability Group (SVG) has been handling software vulnerabilities in Grid Middleware since the start of EGI, and before that a similar activity has been carried out in the EGEE series of projects since 2005. The work is carried out by the SVG "Risk Assessment Team" (RAT). The main principle is that:
* Anyone can report a vulnerability (by e-mail to report-vulnerability@egi.eu)
* The vulnerability is investigated by the RAT, the software provider, and the reporter.
* If the vulnerability is valid a risk assessment is carried out by the RAT.
* A target date for resolution is set according to the risk.

This principle will remain the same after the end of EMI and IGE.
However, much of the current activity depends on agreed contacts with EMI and IGE, and a process agreed with EMI and IGE. By the end of EMI and IGE it will be necessary to establish details of how the process is carried after these projects have ended, including details of who is contacted, and how the middleware and updates are distributed. By the time of the Community forum, this should be established.

Primary author: CORNWALL, Linda (STFC)

Presenter: CORNWALL, Linda (STFC)

Session Classification: Operational Services

Track Classification: Community Platforms (Track Lead: P Solagna and M Drescher)