Contribution ID: **88** Type: **not specified**

The EGI Software Vulnerability Group and EMI

Friday, 30 March 2012 12:00 (25 minutes)

Description of the Work

The purpose of the EGI Software Vulnerability Group (SVG) is to eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware, prevent the introduction of new ones and prevent security incidents.

In order for Vulnerabilities to be resolved they first need to be found. Some members of EMI and EGI and collaborating projects happen to find vulnerabilities and report them to the EGI SVG, and these are handled using a formally agreed process. Some vulnerabilities are found as a result of "Vulnerability assessment" which is the pro-active assessment of software analyse its security. Some of this is done by members of EMI, and EGI SVG and EMI members jointly came up with a plan for which pieces of middleware are assessed and when.

However vulnerabilities are found, they need to be investigated, assessed and eliminated. The investigation and Risk Assessment is carried out by the SVG, whose members are drawn from both EMI and EGI. Since much of the Grid Middleware comes from EMI, then it is often EMI developers who have to actually fix these problems. Co-ordination between EMI and EGI occurs to ensure vulnerabilities are fixed in a timely manner.

Some vulnerabilities are very straight forward, e.g. due to a simple file permission problem, whereas some are more complex and require greater ingenuity from the developers to solve them. Many of the EMI developers are world class security experts and able to find innovative solutions to vulnerability problems.

Conclusions

The EGI SVG in collaboration with EMI has been active in handling, detecting, and eliminating vulnerabilities in the middleware deployed on the EGI infrastructure. There is no way of knowing how many incidents have been prevented by carrying out this work to ensure that the software deployed on the EGI infrastructure is as secure and free from vulnerabilities as possible. It is likely that if vulnerabilities are present someone will exploit them at some time and it is important to remain vigilant. New vulnerabilities and new types of vulnerability are found and with the expanding user base and awareness of the Grid infrastructure it is important to continue these activities to help ensure the security of the Grid.

Impact

As far as we are aware, no security incidents in the EGI infrastructure have so far occurred due to vulnerabilities in Grid Middleware. This probably would not have been the case if it was not for the collaboration between EGI and EMI to eliminate vulnerabilities from the middleware.

Examples of vulnerabilities eliminated may be given, along with an update of the numbers.

Overview (For the conference guide)

This provides a brief overview of the activities of the EGI Software vulnerability Group (SVG), and progress made in collaboration with EMI in addressing software vulnerabilities.
This is followed by a short presentation by 2-3 members of SVG/EMI on how some specific problems occurred and how they were technically addressed.

Primary author: CORNWALL, Linda (STFC)

Presenter: CORNWALL, Linda (STFC)

Session Classification: Security