Contribution ID: **2** Type: **Poster**

Eliminating and preventing Grid Security Vulnerabilities to reduce security risk

Monday, April 12, 2010 5:00 PM (3 minutes)

The EGEE Grid Security Vulnerability Group was formed "to incrementally make the Grid more secure and thus provide better availability and sustainability of the deployed infrastructure". The aim is to eliminate vulnerabilities from the Grid and prevent new ones from being introduced, thus reducing the risk of security incidents. This poster alerts users and developers to both the activities of the this group and problems that may be caused by vulnerabilities. It is also intended to inform what they should do to avoid introducing vulnerabilities and report any their find.

Impact

At the time of writing, over 70 Grid Security Vulnerability bugs have been fixed since the activity started, and several pieces of less secure middleware have been taken out of use as more secure software comes into use.

As far as we are aware, no major Grid Security incident within EGEE or collaborating projects has occured due to a vulnerability in Grid Middleware. This could be due to the fact that we have successfully eliminated many vulnerabilities from the middleware, and successful in preventing new ones. It could also be due to hackers being less alert to Grids that other systems, or that the user community is particularly honest.

Keywords

Grid Security Vulnerability Risk

URL for further information

http://www.gridpp.ac.uk/gsvg/

Detailed analysis

A system for handling Grid Security vulnerabilities was setup in 2006 at the beginning of EGEE-II. A Risk Assessment Team (RAT) was formed which currently has13 members from 10 different institutes to carry out this process, which is:
- anyone may report an issue
- the RAT investigates the issue
- if valid the RAT carries out a Risk assessment putting each issue into 1 of 4 risk categories - Extremely Critical, High, Moderate, or Low.
- a target date for resolution is set according to the risk
- an advisory is issued when the issue is fixed, or on the target date

Certain types of problem occur quite frequently - such as vulnerabilities resulting from incorrect file permissions, or failure to sanitize user input,. Suggestions for how to prevent new vulnerabilities entering the infrastructure will be made.

Some members of the group are currently participating in an 'Overall Security Risk Assessment' which looks at high level risks to the infrastructure, data, and various parties. A summary the reasons for doing this, the strategy, and the outcome (assuming it is available in time) will be included on the poster.

Conclusions and Future Work

A good enthusiastic team has been handling Grid Security Vulnerabilities over the last 4 years, and many vulnerabilities have been eliminated from the deployed infrastructure. New types of vulnerabilities continue to be found and hackers get ever more ingenious in their quest to gain access to sites. This work therefore needs to continue into the future as grid technology increases it's profile and hackers become more alert to this type of system and find new ways of exploiting systems.

Author: Dr CORNWALL, Linda Ann (Particle Physics-Rutherford Appleton Laboratory-STFC - Science &)

Presenter: Dr CORNWALL, Linda Ann (Particle Physics-Rutherford Appleton Laboratory-STFC - Science &)

Session Classification: Poster session

Track Classification: National and international activities and collaborations