

## Description

The Security Assessment Plan identifies which software components are going to be assessed and when the assessments are going to take place.

### Author

- Elisa Heymann - [elisa@csSPAMNOT.wisc.edu](mailto:elisa@csSPAMNOT.wisc.edu)
- Linda Cornwall - [linda.cornwall@stfcSPAMNOT.ac.uk](mailto:linda.cornwall@stfcSPAMNOT.ac.uk)

## Introduction

The University of Wisconsin/Universitat Autònoma de Barcelona Middleware Security and Testing Group have developed and are continuing to develop First Principles Vulnerability Assessment (FPVA) methodology for assessing software for critical vulnerabilities. Assessments of several major middleware systems have been carried out, significant vulnerabilities found in many of them, and the developers helped with remediation strategies. FPVA is being applied to various security related middleware packages supplied by EMI as part of the Quality Control process.

This document describes the plans for this activity, and the current status. A new version will be produced approximately every 3 months as the status changes.

## The Vulnerability Assessment Process

### Principles

#### The 5 main steps

Probably as in the Requirements 5 bullet points on <https://twiki.cern.ch/twiki/bin/view/EMI/SA1QCSA>

#### Details of activities carried out during process

## Description of the communication process

Of the EMI components, so far VOMS Admin 2.0.15 had been assessed using FPVA. Serious vulnerabilities were found and reported to the development team, together with possible fixes. The development team is currently working on fixing the vulnerabilities found. The vulnerabilities are not disclosed yet, but will be after they are fixed and the different user groups have had time to update to the new security release.

## Plans for packages to be assessed during EMI

The nature of the assessment technique means that it is very time consuming, plus only a small number of people are funded to work on this. Hence only a small number of middleware packages can be assessed during the project. Also, before the assessment process gets under way, it is very difficult to estimate the time the assessment process will take, hence it may not be possible to assess all packages planned or it may be possible to do more than originally planned.

The main suppliers of packages within EMI are gLite, ARC, Unicore and dcache.

### Priority

#### gLite

- Argus 1.2. Argus is the gLite Authorization Service. It is intended to provide consistent authorization decisions for distributed services (e.g. compute elements, portals). Argus consists of 3 main components: (a) the Policy Administration Point (PAP) to manage policies; (b) the Policy Decision Point (PDP) to evaluate policies; and (c) the Policy Enforcement Point (PEP) to enforce policy decisions.

Note that a Vulnerability Assessment is already in progress for Argus at the time of writing.

- gLExec 0.8: gLExec provides an identity mapping service. It has been assessed in the past and has since undergone a re-write, mainly to address some of the problems found by these assessments. It is necessary to re-assess the new version, and this is already in progress.
- VOMS Core: It is an Authorization System for Virtual Organizations developed to solve the problems of granting users authorization to access the resources at VO level, providing support for group membership and roles.
- CREAM: It is a job management system for local computational resources. The CREAM (Computing Resource Execution And Management) Service is a lightweight service for job management operation at the Computing Element level. CREAM accepts job submission requests and other job management requests (e.g. job cancellation, job monitoring, etc).
- WMS: It is the gLite Workload Management System, and it is intended for distributing and managing tasks across computing and storage resources available on a Grid.

#### **Unicore**

- TSI: The Target System Interface provides an interface between UNICORE and the individual resource management/batch system and operating system of the Grid resources.
- Gateway: It is an authenticating web proxy service for web service requests (SOAP messages) and normal HTTP traffic of the UNICORE Grid middleware. Is the single entry point for all UNICORE connections into a Usite.

#### **ARC**

??

#### **dCache**

#### **Detailed plan and provisional schedule**

Currently Argus and gLExec are being assessed. These assessments are expected to be finished at the end of March 2011. Argus is being assessed by Manuel Brugnoli (UAB) and gLExec by Daniel Crowell (UWM).

The assessment of VOMS Core will start by April 2011, will be carried out by UAB, and it is expected to take 6 months.

The assessment of CREAM will start by November 2011, will be carried out by UAB, and it is expected to last 6 months.

By May 2012 either TSI or Gateway will be assessed by UAB. The decision depends on what will be determined to be more critical.

#### **Current Status**

Currently the assessment of VOMS Admin is finished, and gLExec and Argus are being assessed. It is expected that both assessments will be finished by the end of March 2011, though as the assessments are carried out manually, it is not possible to establish an exact ending date.

#### **Packages assessed prior to EMI**

Various packages have been assessed using the techniques developed prior to the start of EMI, these include

Condor, SRB (Storage Resource Broker), gLExec, MyProxy, Gratia Condor Probe, Condor Quill, Condor Privilege Separation, and CrossBorker. The assessment of Wireshark is an ongoing effort.

The assessment of VOMS Admin, which is part of EMI is already finished.

### **Packages already assessed during EMI**

VOMS Admin completed on August 2010. Some important issues were found and are currently being addressed by the development team.

### **Packages in Work**

- gLExec
- Argus