PSNC work status

Gerard Frankowski, Rafał Lichwała

Poznań Supercomputing and Networking Center

EGEE SA3 All Hands Meeting, Dublin, December 11-12, 2007

www.eu-egee.org
www.glite.org

Information Society and Media

Security

Gerard Frankowski, Błażej Miga, Tomasz Nowocień
Poznan Supercomputing and Networking Center

SA3 All Hands Meeting, Dublin, December 2007

www.eu-egee.org
www.glite.org

Information Society and Media

RGMA Security audit

- RGMA - Relational-Grid Monitoring Architecture
  - R-GMA is one of the monitoring components that collects and publishes information for further queries, taking into account the dynamic nature of the Grid. As an example a request/resource broker needs information updated to at most the last 10 seconds to be able to distribute/recover the work load in an efficient way.
  - org.glite.server-servlet component

RGMA Security audit

- **Testbed specification**
  - **Hardware:**
    - **IBM ThinkPad T23 (256MB RAM, Mobile Intel® Pentium® III CPU – M 1133MHz)**
  - **Software:**
    - **Linux Gentoo – kernel 2.6.17-gentoo-r8**
    - **Gcc version: 4.1.1**
    - **Globus 4.0.1-VDT-1.3.10**
    - **Openssl 0.9.7j**
    - **Tomcat 5.0.27-r6**
    - **Mysql Ver 14.12 Distrib 5.0.27**
    - **glite-RGMA-server-servlet-5.0.43-1.noarch.rpm**

RGMA Security audit - results

- **XSS (Cross Site Scripting)**
  - File: /src/org/edg/info/BrowserServlet.java
  - Code:

```
String[] cols =
m_schemaBrowser.getColumnStrings(tableName);
if (cols != null) { ... }
else {
 buffer.append("table name <b>" + tableName +
 "</b>");
 buffer.append("cannot be found in R-GMA.");
}
```

  - Example:

    https://localhost:8443/R-GMA/BrowserServlet/getQueryForm.do?tableName=<script>alert(1)</script>

RGMA Security audit - results

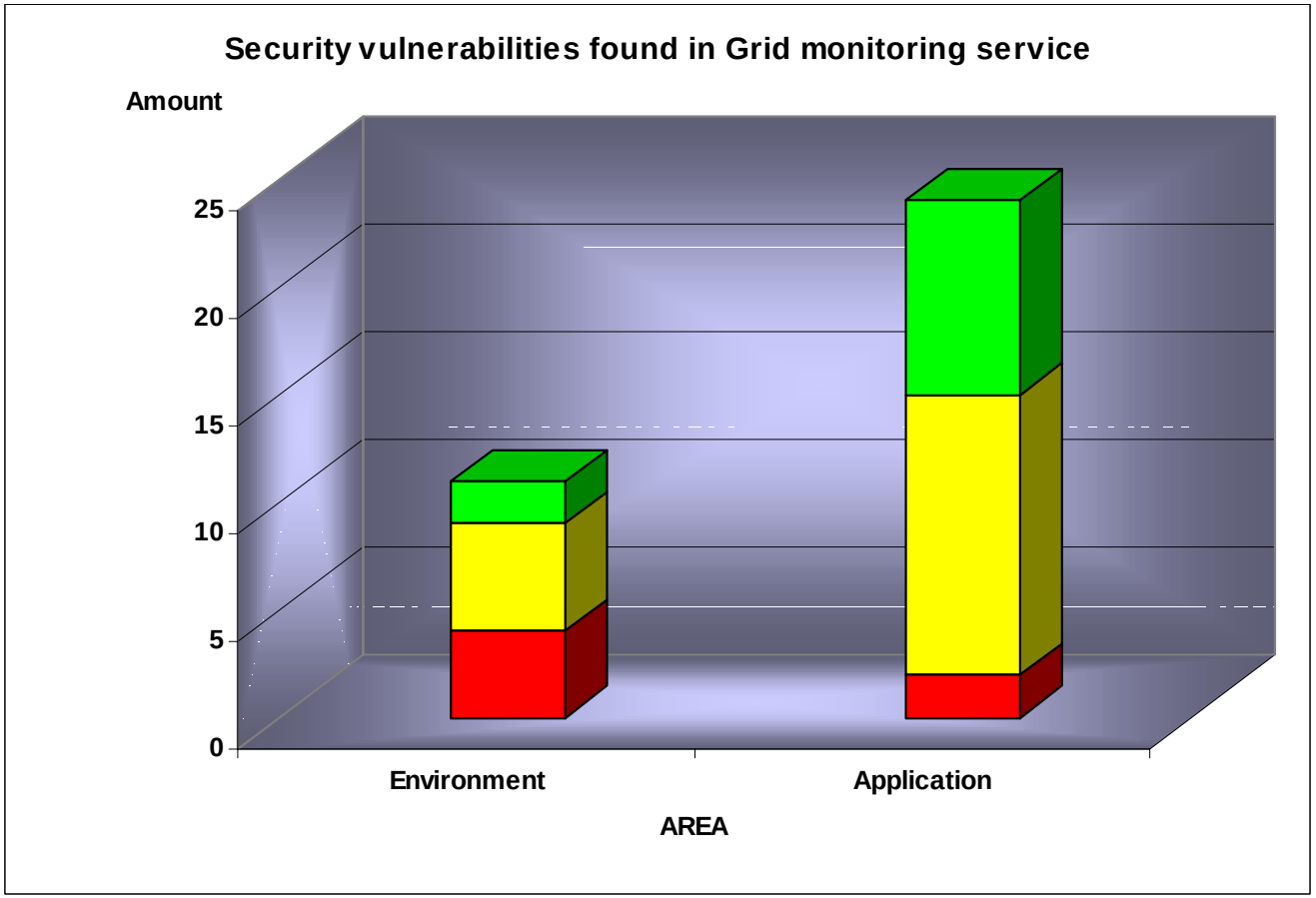
- **SQL Injection:**
  - File: /src/org/edg/info/BrowserServlet.java
  - Example:
    - https://localhost:8443/R-GMA/BrowserServlet/getTableInfo.do?tableName=123'%20union%20select%20'1231232222222222222222222222222
    - https://localhost:8443/R-GMA/BrowserServlet/getQueryForm.do?tableName=123'%20union%20select%20'123123222222222222222222222
- **Report issued**

Grid monitoring service audit

- **http://monitoring.egee.man.poznan.pl**
- **Methodology**
  - 1st stage: *black box* testing
  - 2nd stage: *crystal box* testing
- **Testbed**
  - None – productive environment
  - Crystal box: including local analysis of the source code
- **Technologies under investigation**
  - Apache Web Server
  - PHP + MySQL
  - PHP-written libraries: JPGraph, LDAP Explorer
- **Tools**
  - Burp suite (Burp proxy, Burp spider)
  - Source code analyzers: pixy, RATS
  - Manual source code analysis: grep & text editors

Results

- **Two separate areas**
  - Application environment (OS, Web Server, PHP, MySQL, …)
  - The application itself



Found vulnerabilities

- **Source code vulnerabilities**
  - Remote Code Execution
  - XSS
  - SQL Injection
  - Directory Traversal
  - Information Disclosure
- **Application environment vulnerabilities**
  - Versions of software components
  - Contents of configuration files

Remote code execution

- **Remote code execution**
  - File: http://monitoring.egee.man.poznan.pl/jobs/ping.php
  - Code:

```
$host = $_GET['host']
... //no validation of $host
passthru ("ping -c 5 $host");
```

  - Attack 1:
    - http://monitoring.egee.man.poznan.pl/jobs/ping.php?host=www.onet.pl;ls%20/etc/passwd
  - Attack 2:
    - works even after securing the function with escapeshellcmd()
    - http://monitoring.egee.man.poznan.pl/jobs/ping.php?host=www.onet.pl%20-c%209999%20-s%2065510

Reading system files

- **Reading (almost) arbitrary files**
  - File: http://monitoring.egee.man.poznan.pl/ldap/php/tree.php
  - Code:

```
$fileID = $_REQUEST['fileID'];
... //no validation of $fileID
$fullcontent = file ($tmpdir . $fileID);
```

  - The $fullcontent is then processed in various ways
  - Example:
    - **Capture the request:**

      GET /ldap/php/tree.php?actionID=expand&fileID=tmp/LEOO331mUA&row=2&...
    - **Craft the request to:**

      GET /ldap/php/tree.php?actionID=expand&fileID=../../../../../../etc/passwd&row=2&...
    - **See the contents of the file:**

      http://monitoring.egee.man.poznan.pl/ldap/php/tmp/LEOO331mUA

Output and recommendations

- **Output**
  - Full report for EGEE
  - Internal PSNC report (No. 6/2007) – in Polish
  - Help for building *best practices* document
- **Recommendations**
  - **Always** filter the user input
    - Avoid accepting HTML tag characters < and >
    - Always apply quotations for parameters in database queries
    - Take care when calling external programs
    - Filter the database **output** as well!
  - Be careful with the software versions and updates
  - Don’t use components with security vulnerabilities
  - Apply appropriate configuration of software components

Security best practices

- **Defence in depth**
  - Everyone must care
- **2 parts:**
  - For developers
  - For administrators
- **The document will contain (but will not be limited to) some recommendations from the Grid monitoring application security audit**

TODO

- **The nearest schedule for security:**
  - Dec 2007: VOMS server instance – verifying old vulnerabilities
  - Dec 2007 / Jan 2008: LFC – security tests report
  - Dec 2007 / Jan 2008: *Best practices* document
  - Dec 2007 / Jan 2008: VOMS test scripts

Porting

Rafał Lichwała, Adrian Stelmaszyk

Poznan Supercomputing and Networking Center

SA3 All Hands Meeting, Dublin, December 2007

Porting – current status

- Etics bug that has been reported – fixed;
- Etics Client version: 1.2.3-1;
- Two main steps before we will be able to build a first Debian-4 x86_64 gLite WN package:
  - Preparing open source externals in Etics repository;
  - Building and preparing VDT externals;
- ... then we should start the real porting... :)

Open source externals

- Most of them have their equivalents for Debian-4 x86_64
- Sometimes small modifications have been needed:
  - package renaming
  - removing unnecessary libraries
  - modification of directory tree structure
- All those externals have been installed and prepared for Etics repository as binary packages for debian4 platform

VDT externals

- VDT does not support Debian4 – They "... plan to build it for VDT 1.8.2 in a couple of months..."
- We decided to prepare our own VDT packages:
  - building VDT 1.8.1 on Debian basing on pacman and x86_64 packages from RHEL-5
  - process failed – problem has been reported to VDT Team – no solution till now...
  - successful installation from RHEL-4 but many packages not fully compatible with the required libraries – process abandoned
  - Preparing for VDT building from sources – in progress...

Comments, questions...

Thank you for your attention!

gerard@man.poznan.pl
(Security)
syriusz@man.poznan.pl
(Porting)