Sensitive information disclosure in the RESTX framework

Security advisory
09/03/2016

Julien Legras
The RESTX framework

RESTX is a Java REST framework. It provides an easy way to build RESTful API with methods annotation. An administration web console is also available. It allows the administrator to read the API documentation and specifications and to manage the RESTX configuration.

The administration web console is an AngularJS application running inside the web browser. It requests REST administration endpoints to populate the pages.

The issues

Synacktiv has identified vulnerabilities in the security mechanism that protects sensitive resources such as the configuration content. When a user tries to request a REST endpoint that does not exist, the server returns the entire routes list:

```
no restx route found for GET /test
go to http://192.168.56.104:8080/api/@/ui/api-docs/ for API documentation
```

```
GET /message => default#HelloResource#sayHello
GET /hello => default#HelloResource#helloPublic
GET /@/sources/resources/{path:*} => FS:/home/user/restx-samples-hello/src/main/resources
PUT /@/sources/resources/{path:*} => FS:/home/user/restx-samples-hello/src/main/resources
DELETE /@/sources/resources/{path:*} => FS:/home/user/restx-samples-hello/src/main/resources
GET /@/sources/main/{path:*} => FS:/home/user/restx-samples-hello/src/main/java
PUT /@/sources/main/{path:*} => FS:/home/user/restx-samples-hello/src/main/java
DELETE /@/sources/main/{path:*} => FS:/home/user/restx-samples-hello/src/main/java
GET /@/pages => restx-admin#AdminPagesResource#findPages
GET /@/api-docs/schemas/{fqcn} => restx-admin#JsonSchemaResource#getJsonSchema
GET /@/specs => restx-admin#SpecsResource#findSpecsForOperation
GET /@/specs/{id} => restx-admin#SpecsResource#getResource
PUT /@/specs/{id}/wts/{wsiIndex}/then => restx-admin#SpecsResource#updateSpecThenHtip
GET /@/config/elements => restx-admin#ConfigResource#findConfigElements
```

From this list, Synacktiv tried to access /@/ui/config/ but the application redirects the user to the administration login page. However, this redirection is actually done by the AngularJS application, in the web browser. This application requests 2 sensitive resources:

- /@/pages : returns 403
- /@/config/elements : returns 200 and its content if a valid session cookie is provided (but admin role not needed)

As an application needs to have a valid session cookie in order to perform REST requests, it means that anyone who can steal the session cookie can access the server configuration including:

- administrator password,
- database credentials,
- database IP address,
- etc.

The vulnerability can be exploited in the first sample application restx-samples-hello with the user user1 that is allowed with the role hello, specific to this sample application and not related to the admin role:
Almost all administration modules resources are affected by this vulnerability.

**Affected versions**

The versions up to 0.34 of the following modules are vulnerable:

- `restx-admin (/@/config/elements)`
- `restx-log-admin (/@/ui/log)`
- `restx-stats-admin (/@/restx-stats)`
- `restx-monitor-admin (/@/sessionStats, /@/metrics, /@/health-checks, /@/thread-dump)`
- `restx-factory-admin (/@/warehouse, /@/factory)`

**Mitigation**

The RESTX version 0.34.1 fixes the issues.
## Timeline

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>15/01/2016</td>
<td>Advisory sent to the main developer, but no answer</td>
</tr>
<tr>
<td>31/01/2016</td>
<td>Second e-mail sent to other developers of the project</td>
</tr>
<tr>
<td>31/01/2016</td>
<td>Acknowledgment from the team</td>
</tr>
<tr>
<td>08/02/2016</td>
<td>Fix pushed on the github repository</td>
</tr>
<tr>
<td>09/03/2016</td>
<td>Advisory published by Synacktiv</td>
</tr>
</tbody>
</table>