



...making excellence a habit.™

Security Assessment Report

Dragon InfoSec
Blockchain

BSI Reference: IA141113-RPT-01

Version: 1.0

12th July 2018

Testing Team

Mark Woan



Document Control Information**1.1 Document Details**

Property	Value
Client	Dragon InfoSec
Title	Blockchain Security Assessment Report
Author	Mark Woan
Version	1.0
Date	12/07/2018
Document Reference	IA14113-RPT-01
Status	Final

1.2 Revision History

Version	Date	Author	Summary of Changes
0.1	12/07/2018	Mark Woan	Initial Draft
0.2	18/07/2018	Christian Hobbs	Internal QA
1.0	18/07/2018	Christian Hobbs	Definitive Issue

1.3 Approvals

Name	Organisation	Role
Peter Viranyi	BSI Cybersecurity and Information Resilience	Head of Security Testing

1.4 Distribution

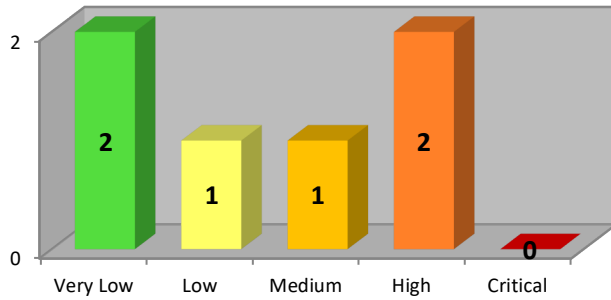
Name	Organisation	Role
Martin Walsham	BSI Cybersecurity and Information Resilience	Information Security Director
Richard Dennis	Dragon InfoSec	CTO

Table of Contents

- DOCUMENT CONTROL INFORMATION 2**
- 1.1 Document Details 2
- 1.2 Revision History 2
- 1.3 Approvals..... 2
- 1.4 Distribution 2
- 2 EXECUTIVE SUMMARY..... 4**
- 3 INTRODUCTION 5**
- 3.1 Approach 5
- 3.2 Scope 5
- 4 RESULTS OF ASSESSMENT 6**
- 4.1 API Lacks Authentication 6
- 4.2 Negative Transaction Amount Not Validated 7
- 4.3 API Access Over a Cleartext Protocol..... 8
- 4.4 Wallet Secrets Unencrypted 9
- 4.5 Transaction Amount Validation 10
- 4.6 NIST Beacon Signature Check Value Not Used 11
- 5 SUMMARY OF FINDINGS 12**
- 5.1 Results of Assessment..... 12
- APPENDIX A - TESTING TEAM 14**
- APPENDIX B - FINDINGS DEFINITIONS 15**

2 Executive Summary

BSI Cybersecurity and Information Resilience were engaged by Dragon InfoSec to perform a security assessment against their custom blockchain implementation. Testing was undertaken remotely between the 5th and 12th of July 2018.



This graph illustrates the level of risk that was identified within the implementation. It shows the number of issues identified during this assessment along with their severity.

As can be seen from the graphs above, high areas of risk have been identified within the environment.

The high and medium risk issues are summarised as the following:

The first high risk issue was the lack of authentication when accessing the remote API located on the server nodes. An attacker would be able to perform actions such as creating transactions to transfer funds between wallets. The API is not published externally and therefore an attacker would have to determine the correct format of the commands before being able to perform any actions. The second-high risk issue was the lack of input validation when creating a transaction, by supplying invalid transaction amount values, it was possible to transfer funds from the receiving wallet into the sender’s wallet. This issue was fixed during the testing phase, and the fix validated to ensure that the issue was resolved.

The medium risk issue was the lack of encryption when communicating with the remote API on the node servers. An attacker in a position to eavesdrop on the communication between an end user and the server would be able to see the commands and data sent to the API. This issue will have a greater impact when the authentication is implemented for accessing the API.

It is noted that the development of the blockchain implementation is ongoing, and that some of the issues are due to the current level of implementation.

3 Introduction

BSI Cybersecurity and Information Resilience were engaged by Dragon InfoSec to perform a security assessment against their custom blockchain implementation. Testing was undertaken remotely between the 5th and 12th of July 2018.

3.1 Approach

All testing was carried out using BSI Cybersecurity and Information Resilience standard testing methodology. A full copy of this methodology can be provided on request.

3.2 Scope

The scope of the engagement was as follows:

- Perform a double spend
- Inject a malicious transaction into the blockchain
- Generate the private key from its associated public key
- Delete a transaction from the blockchain
- Assess the public API
- Assess the cryptographic routines used for address generation
- Assess the security of the NIST time beaconing
- Assess the implementation of the blockchain storage

3.2.1 Limitations



The following limitations were identified:

- The blockchain implementation was still in an early development phase, and therefore other issues may arise as the implementation continues

4 Results of Assessment

This section provides the detailed findings of the assessment that was performed between the 5th and the 12th July 2018.

4.1 API Lacks Authentication

Finding No 1.	Systems Affected	
	Finding	The API used to interact with blockchain did not require the user to authenticate before performing actions.
	CVE Number	N/A
	Root Cause	Web Development
	Impact	4 
	Likelihood	4 
	Overall Risk Rating	16 (High Risk)
	Status	ONGOING

4.1.1 Summary

The server-based API used to interact with blockchain did not require the user to authenticate before performing any actions.

4.1.2 Technical Details

The server based API has various methods that allow the user to perform actions such as creating a new transaction, creating a new wallet and retrieving a wallet balance. The API is accessed via the HTTP protocol. The API does not require the user to authenticate before performing any actions.

4.1.3 Recommendation

BSI recommends that the API be modified to require users to authenticate before being permitted to interact with the blockchain, network and wallets. Examples of authentication methods that could be implemented include username/password, JSON Web Tokens and certificate based authentication.

4.2 Negative Transaction Amount Not Validated

Finding No 2.	Systems Affected	
	Finding	It was possible to take funds from other user's wallets and bypass wallet balance checks by using negative amount values when creating a transaction
	CVE Number	N/A
	Root Cause	Web Development
	Impact	4
	Likelihood	4
	Overall Risk Rating	16 (High Risk)
	Status	RESOLVED

4.2.1 Retest Status

This issue was validated during the original testing phase and found to be resolved.

4.2.2 Summary

It was possible to take funds from other user's wallets and bypass wallet balance checks by using negative amount values when creating a transaction to transfer funds from one address to another.

4.2.3 Technical Details

It was possible to provide negative values to the **amount** JSON value in the **/transaction/create** API call, which resulted in the **amount** being deducted from the receiving wallet, rather than the sending wallet.

It was also possible to request a negative amount that was greater than either the receiving or sender wallet balances e.g. -1000, when the sender has a balance of 100, and the receiver a balance of 10. The result of which would be that the sender would receive a credit of 1000 and have a balance of 1010.



An example **curl** command used to test the issue is shown below:

```
curl -H "Content-type: application/json" --data '{"from":
"04f442bcc674bc4399c30cf5e9c40892d6f59a7aa8a69e5df8409232cb4173b82744a1265295a057120d0e953dd8ad79f
32865b4b582a6eb1bab81623520950d66", "to":
"0405b8831608221b8c149e1f9ecc24d19cb356d56ee4c54dbbfb679d7576b4e5693585d8da24c8182ba4c6913c5e6bf0c
60bb85eaca06cf07055f3bef421781d20", "amount": -1000}' http://54.38.214.253:3001/transaction/create
```

4.2.4 Recommendation

BSI recommends that the application be modified to validate all user supplied input and in particular the **amount** value sent to the **/transaction/create** API call.

4.3 API Access Over a Cleartext Protocol

Finding No 3.	Systems Affected	
	Finding	The server based API was accessible over the unencrypted HTTP protocol
	CVE Number	N/A
	Root Cause	Configuration
	Impact	4 
	Likelihood	2 
	Overall Risk Rating	8 (Medium Risk)
	Status	ONGOING

4.3.1 Summary

The server based API was accessible over the unencrypted HTTP protocol.



4.3.2 Technical Details

By using cleartext protocols for communications a risk exists whereby an attacker that is suitably positioned can read the traffic traversing the network between the servers and connecting devices.

4.3.3 Recommendation

BSI recommends that an encrypted transport channel for all client/server communications, such as SSL/TLS, is enforced.

4.4 Wallet Secrets Unencrypted

Finding No 4.	Systems Affected	
	Finding	The secret values associated with each wallet address were stored in a clear text JSON file
	CVE Number	N/A
	Root Cause	Web Development
	Impact	2 
	Likelihood	2 
	Overall Risk Rating	4 (Low Risk)
	Status	ONGOING

4.4.1 Summary

The secret values associated with each wallet address were stored in a clear text JSON file.

4.4.2 Technical Details



The secret values associated with each wallet address are used in conjunction with the Elliptic Curve Digital Signature Algorithm (ECDSA) to sign transactions within the blockchain. Due to the centralised nature of this blockchain implementation, the impact of an attacker having knowledge of an addresses secret key would be minimal. The transactions are created on the server nodes using the API, each server node has to validate before it is permitted to connect to the network, therefore manipulation of the blockchain would have to occur directly on the server, rather than via the API.

If an attacker gained control of a node they would potentially have access to all wallets on the server, so an attack that created a rogue transaction using the secret value to sign the transaction would have far less impact.

4.4.3 Recommendation

BSI recommends that the server implementation be modified to store the wallet details in an encrypted format, and the details decrypted at runtime where required.

4.5 Transaction Amount Validation

Finding No 5.	Systems Affected	
	Finding	Invalid transaction Amount Values Server Errors
	CVE Number	N/A
	Root Cause	Web Development
	Impact	1 
	Likelihood	2 
	Overall Risk Rating	2 (Very Low Risk)
	Status	ONGOING

4.5.1 Summary

Submitting double negative transaction **amount** values (--10) caused unexpected server errors.

4.5.2 Technical Details

When double negative transaction **amount** value (--1) was submitted to the **/transaction/create** API, the server returned a HTTP 400 (Bad Request) response, with the response body containing the following message:

The sender does not have enough to pay for the transaction.

The response returned by the application differs from that when supplying a negative amount (-1), which was a HTTP 500 status code, with the response body containing the following message:



Internal Server Error

The error message regarding the lack of funds indicates that the double negative amount value is passing through to the point of creating a transaction, rather than being identified within the HTTP server functionality providing the API.

4.5.3 Recommendation

BSI recommends that the application be modified to validate all user supplied input and in particular the **amount** value sent to the **/transaction/create** API call. Invalid values should be rejected rather than sanitized.

4.6 NIST Beacon Signature Check Value Not Used

Finding No 6.	Systems Affected	
	Finding	The beacon responses public key is validated by the application; however, invalid signatures are not rejected.
	CVE Number	N/A
	Root Cause	Web Development
	Impact	1 
	Likelihood	2 
	Overall Risk Rating	2 (Very Low Risk)
	Status	ONGOING

4.6.1 Summary

The NIST beacon signature hash value is used to determine which node performs the mining function for a period of one minute. The application validates that the beacon response is signed using the published public key, however, it appears that regardless of whether the signature is valid or not, the beacon signature hash value is used.

4.6.2 Technical Details

The NIST beacon prototype implementation generates full-entropy bit-strings and posts them in blocks of 512 bits every 60 seconds. Each such value is sequence-numbered, time-stamped and signed, and includes the hash of the previous value to chain the sequence of values together and prevent even the source to retroactively change an output package without being detected. The beacon signature hash value is used to determine which node performs the mining function for a period of one minute.

The application validates that the beacon is signed using the published public key, however, it appears that regardless of whether the signature is valid or not, the beacon signature hash value is used.

It is thought that the only impact of controlling the beacon signature value would be to control which node performed the mining function for the one-minute period.

4.6.3 Recommendation

BSI recommends that the application be modified to reject beacon requests where the signing validation fails.

5 Summary of Findings

5.1 Results of Assessment

Finding No.	Impact	Likelihood	Overall Risk	Finding	Recommendation	Status
1	4	4	High	API Lacks Authentication The API used to interact with blockchain did not require the user to authenticate before performing actions.	BSI recommends that the API be modified to require users to authenticate before being permitted to interaction with the blockchain, network and wallets. Examples of authentication methods that could be implemented include username/password, JSON Web Tokens and certificate based authentication.	ONGOING
2	4	4	High	Negative Transaction Amount Not Validated It was possible to take funds from other user's wallets and bypass wallet balance checks by using negative amount values when creating a transaction to transfer funds from one address to another.	BSI recommends that the application be modified to validate all user supplied input and in particular the amount value sent to the /transaction/create API call.	RESOLVED
3	4	2	Medium	API Access Over a Cleartext Protocol The server based API was accessible over the unencrypted HTTP protocol	BSI recommends that an encrypted transport channel for all client/server communications, such as SSL/TLS, is enforced.	ONGOING
4	2	2	Low	Wallet Secrets Unencrypted The secret values associated with each wallet address were stored in a clear text JSON file	BSI recommends that the server implementation be modified to store the wallet details in an encrypted format, and the details decrypted at runtime where required.	ONGOING

Finding No.	Impact	Likelihood	Overall Risk	Finding	Recommendation	Status
5	1	2	Very Low	Transaction Amount Validation Submitting double negative transaction amount values (--10) caused unexpected server errors.	BSI recommends that the application be modified to validate all user supplied input and in particular the amount value sent to the /transaction/create API call. Invalid values should be rejected rather than sanitized.	ONGOING
6	1	2	Very Low	NIST Beacon Signature Check Value Not Used The beacon responses public key is validated, however, invalid signatures are not rejected.	BSI recommends that the application be modified to reject beacon requests where the signing validation fails.	ONGOING

Appendix A - Testing Team

This project was undertaken using the following consultant:

- Mark Woan

Any queries regarding this testing and report should be directed to:

BSI Cybersecurity and Information Resilience Operations Team

Tel: +44 (0) 345 222 1711

Email: Operations.Cyber.UK@bsigroup.com

The primary point of contact at Dragon InfoSec was Richard Dennis (richard@dragoninfosec.com).

Appendix B - Findings Definitions

BSI Cybersecurity and Information Resilience have developed a method for evaluating vulnerabilities and presenting the results in a way which enables clients to easily assess the risks they pose to the organisation.

B.1. Risk Ratings

Each finding is categories by its "Seriousness" and "Likelihood". The overall risk rating is calculated as a multiple of the two values.

$$\text{Overall risk} = \text{Seriousness} \times \text{Likelihood}$$

Below are guidance on rating definitions; exact ratings may depend on particular environment.

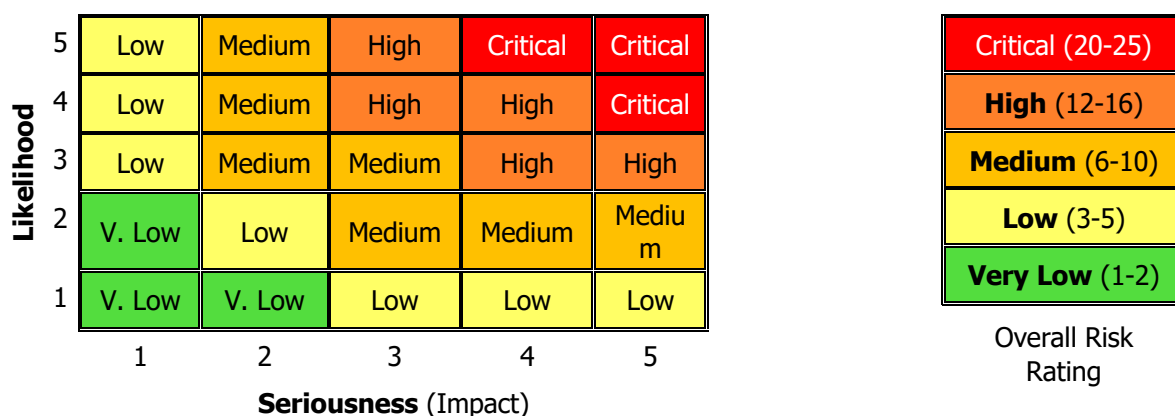
Seriousness (Impact)

- 5** - Remotely gaining administrative access;
- 4** - Remote privilege escalation or unauthorised read/write access;
- 3** - Local privilege escalation or unauthorised read-only access to data;
- 2** - Sensitive information disclosure. Minor security configuration weakness;
- 1** - Minor non-sensitive information disclosure.

Likelihood (exploitability)

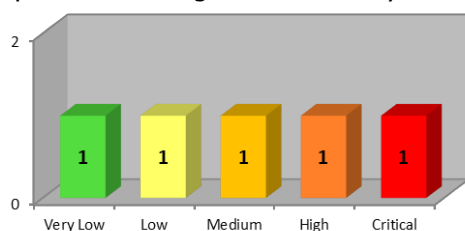
- 5** - Trivial to exploit by unskilled person;
- 4** - Require exploit code or tool which was in the public domain, or easy to exploit with some knowledge;
- 3** - Require some exploit code development or effort to exploit, or require specific knowledge/skill;
- 2** - Attacker may require specific access;
- 1** - Theoretical vulnerability where there is no known exploit code and/or would require a lot of resources to exploit.

Rating may also take in to account existing defences which may restrict the exploitability.



B.2. Executive Summary

The executive summary provides a number of graphical representations as to the most common root cause of the vulnerabilities identified. A summary of the number of different root cause categories are summarised in a graph in the management summary.



In addition, all findings are plotted onto a graph so that the severity of the vulnerabilities identified can easily be visualised. This enables the client to concentrate their efforts for resolution in specific areas

B.3. Findings Box

The table below provides a key to understand the findings description.

Finding No. X	Systems Affected	List of devices which are vulnerable. This will either take the form of IP addresses (DNS names) or URLs.
	Finding	An overview of the vulnerability identified.
	CVE number	Where possible, references will be made to a common reference identifier such as CVE or CWE. These references to external sources allow clients to find out additional details regarding the vulnerability and how to mitigate it.
	Root Cause	Each finding will be categorised as to the perceived root cause. Further details are discussed in the section below.
	Seriousness (Impact)	Impact if the vulnerability is successfully exploited. Rated from 5 (serious) to 1(not serious). <div style="display: flex; align-items: center; justify-content: center; margin-top: 10px;"> <div style="margin-right: 10px;"> 5 - ■ ■ ■ ■ 4 - ■ ■ ■ ■ 3 - ■ ■ ■ ■ 2 - ■ ■ ■ ■ 1 - ■ ■ ■ ■ </div> <div style="margin-left: 20px;">(visual representation)</div> </div>
	Likelihood	How easy is the vulnerability to exploit? Ratings from 5 (easy) to 1 (difficult).
	Overall Risk rating	The overall risk rating takes into account the seriousness of the issue, the likelihood of the vulnerability being exploited, as well as other factors that could impact the overall risk.

Note: It should be noted that the definitions defined above for the seriousness and likelihood ratings are only guidelines.