Digital Security

БЕЗОПАСНОСТЬ КАК ИСКУССТВО

CONFIDENTIAL

EXPERT REPORT

on the results of security assessment
and stress testing of PoA.Network

Timeframe:
7.12.17- 13.12.17
Project manager:
Pertsev A.O.
Head of Audit department:
Tyurin A.N.

Table of Contents

1. Introduction

1.1. General provisions

This expert report contains the results of security assessment and stress testing of Proof-of-Authority Network (hereinafter referred to as “the System”) owned by PoA.Network (hereinafter referred to as “the Company”) with recommendations on the current security level improvement.

1.2. Generally accepted abbreviations

Table 1.2–1. Generally accepted abbreviations

Abbreviation	Meaning
IS	Information security
DS	Data system
SW	Software
PoA	Proof-of-Authority
DOS	Deny of Service

1.3. Abstract

According to the Agreement № DSS-SC-2017/38 dd. 04.12.2017, “Digital Security” experts conducted a security assessment and stress testing of the System in the period of 07.12. 2017 – 13.12.2017.

In the scope of work, they used and examined the external attacker model.

The performed work indicated that an external attacker could use the vulnerability described in the par. 3.2.3. to identify actual IP addresses of all the validators (miners) existing in the System and disrupt the network by conducting a 3 Gbit/s DOS attack (see par. 4.2.1.).

Main recommendations:

1. Mitigate detected technical vulnerabilities;
2. Mitigate detected architectural vulnerabilities.

The text below contains the details on detected vulnerabilities, IS impacts related to them and recommendations on mitigation of the vulnerabilities.

1.4. Audit scope

In the scope of the audit, “Digital Security” experts checked the Company’s hosts listed in the table below (see Table 1.4.).

Table 1.4. Hosts list

№	IP address	Function/Purpose/Name
1	35.167.241.12	red-netstats.poa.network
2	34.216.117.87	Bootnode-1
3	34.208.23.103	Bootnode-2
4	34.216.147.105	Client-1
5	52.42.23.162	Client-2
6	52.33.190.107	Client-3
7	35.163.139.115	Client-4
8	52.26.190.40	red-explorer.poa.network
9	35.166.168.95	Master of Ceremony
10	35.167.218.240	Validator-1
11	34.208.40.21	Validator-2
12	104.20.34.254	red.poa.network (balancer)

2. Audit principles

2.1. IS threats

There are 3 types of IS threats that can affect the Company's information resources: violations of confidentiality, integrity or availability of information.

Confidentiality violation is usually aimed at information disclosure. If a violation is successful, the information becomes known to people, who should not have access to it: unauthorized personnel of the Company, clients, partners, competitors, and third parties.

Integrity violation is aimed at modification or corruption of the information, which can lead to modification of its structure or content, and to a complete or partial destruction of the data.

Availability violation (denial-of-service threat) involves data system users' inability to access the information.

The core principle of this IS audit is an estimation of exploitation likelihood of the aforementioned threats affecting the Company's information resources, within the framework of a pre-defined attacker model.

2.2. Attacker model

A potential attacker is an individual or a group of individuals, acting either in collision or independently, whose intended or unintended actions can carry the aforementioned threats to the IS, infringe information resources of the System or negatively affect the Company's interests.

IS threats are basic threats to confidentiality and integrity of information and the threat of the System denial-of-service.

Attackers can pursue the following goals (and their possible combinations):

- cause Denial of Service;
- escalate their privileges in the System;
- get unauthorized access to business-critical data.

In the scope of work, "Digital Security" experts used an external attacker model

2.2.1. External attacker

The following submodel of an external attacker model was used to conduct the audit:

- an external attacker is an anonymous Internet attacker that has knowledge of the tested System obtained from public sources but has no privileges in it.

3. External analysis of the System

3.1. Detected vulnerabilities

3.1.1. Outdated server software

Severity: medium
Likelihood of exploitation: medium
Overall impact level: medium

Description:

One of the System components is outdated software that contains a lot of common vulnerabilities.

Impact:

An attacker can conduct successful attacks of different types on the Company's web server and other outdated software. The consequences vary according to the type of an exploited vulnerability.

Vulnerable resources:

- red-netstats.poa.network
- red-explorer.poa.network

Technical details:

Publicly available packages.json of the chain-explorer and eth-netstats applications indicate the use of outdated components (modules), most of which contain critical vulnerabilities.
Sources of package.json:

- github.com/oraclesorg/chain-explorer/blob/master/package.json
- github.com/oraclesorg/eth-netstats/blob/master/package.json

Recommendations:

- Update software to the latest versions;
- Implement the process of systematic server software updating.

3.1.2. Debugging information read-out vulnerability

Severity: low
Likelihood of exploitation: medium
Overall impact level: low

Description:

Debugging information read-out is allowed in case of a system failure.

Impact:

Judging from server responses, an attacker can identify a version of system software, used classes, an installation path of a web application, and, consequently, use this information to perform targeted attacks.

Vulnerable resource:

- red-netstats.poa.network

Technical details:

By default, expressjs of the 4.13.3 version attempts to process the body of an HTTP request regardless of an HTTP method. The example below demonstrates how expressjs tries to process the body of the json request. It results into an error because the body is empty.
Request:

```
GET / HTTP/1.1
Host: red-netstats.poa.network
Content-Length: 4
```

Response:

```
HTTP/1.1 400 Bad Request
Date: Fri, 08 Dec 2017 21:31:47 GMT
Content-Type: text/html; charset=utf-8 Connection: keep-alive
Set-Cookie: __cfduid=d33ede4ec2cc4f65840e011f27642cfac1512768706; expires=Sat,
08-Dec-18 21:31:46 GMT; path=/; domain=.poa.network; HttpOnly
X-Powered-By: Express
Server: cloudflare-nginx CF-RAY: 3ca2d55fcbf08625-ARN
Content-Length: 1297

<!DOCTYPE html><html ng-app="netStatsApp"><head><meta name="viewport"
content="width=device-width, initial-scale=1.0, maximum-
scale=1.0"><title>Ethereum Network Status</title><style
type="text/css">[ng\:cloak], [ng-cloak], [data-ng-cloak], [x-ng-cloak], .ng-
cloak, .x-ng-cloak { display: none !important; }</style><link rel="stylesheet"
href="//fonts.googleapis.com/css?family=Source+Sans+Pro:200,300,400,600,700"><li
nk rel="stylesheet" href="/css/netstats.min.css"></head><body><h1>invalid
json</h1><h2>400</h2><pre>Error: invalid json     at parse (/home/netstat/eth-
netstats/node_modules/body-parser/lib/types/json.js:83:15)     at
/home/netstat/eth-netstats/node_modules/body-parser/lib/read.js:108:18     at
invokeCallback (/home/netstat/eth-netstats/node_modules/raw-
body/index.js:262:16)     at done (/home/netstat/eth-netstats/node_modules/raw-
body/index.js:251:7)     at IncomingMessage.onEnd (/home/netstat/eth-
netstats/node_modules/raw-body/index.js:307:7)     at emitNone
(events.js:106:13)     at IncomingMessage.emit (events.js:208:7)     at
endReadableNT (_stream_readable.js:1056:12)     at _combinedTickCallback
(internal/process/next_tick.js:138:11)     at process._tickCallback
(internal/process/next_tick.js:180:9)</pre><script
src="/js/netstats.min.js"></script></body></html>
```

Recommendations:

- Disable debugging information read-out.
- Update Expressjs server.

3.1.3. Denial of Service

Severity: medium
Likelihood of exploitation: high
Overall impact level: high

Description:

An attacker can cause Denial of Service of a service.

Impact:

Denial of Service of the Explorer service may lead to unavailability of information about an account status and network transactions for a user.

Vulnerable resource:

- red-explorer.poa.network

Technical details:

All the requests that are related to acquiring data from blockchain may be used to conduct a DOS attack. Below you can find an example of a request to retrieve transaction data.
Request:

```
GET /tx/<ARBITRARY HASH>
HTTP/1.1
Host: red-explorer.poa.network
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101
Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-
Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://red-explorer.poa.network/
Cookie: __cfduid=d918753434596401f7f62e445947271e51512753733
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 0
```

If a request is repeated from one and the same host in 30 or more streams, the service becomes unavailable for a user.

Recommendation:

- Implement the CAPTCHA mechanism for time-consuming requests.

3.2. Detected security weaknesses

3.2.1. Information disclosure (1)

Description:

Any network participant can disclose IP addresses of other users in the network.

Impact:

An attacker can use the obtained information to perform further attacks.

Vulnerable resourse:

- poa.network

Technical details:

All the IP addresses in a network can be obtained by the following command:

```
curl --data '{"method":"parity_netPeers","params":[],"id":1,"jsonrpc":"2.0"}' -H
"Content-Type: application/json" -X POST localhost:8545 -s | jq
'.result.peers[]' | jq '.network.remoteAddress' | cut -d "\"" -f 2 | cut -d ":"
-f 1
```

3.2.2. Information disclosure (2)

Description:

A parity-client and a web server are deployed on the same host, i.e., the web service can be detected in the network.

Impact:

An attacker can identify IP addresses of web resources stored in the network (Explorer web) and attack them.

Vulnerable resource:

- red-explorer.poa.network

Technical details:

Having obtained the list of IP addresses of network participants, an attacker can scan the list to find open ports and, consequently, impersonate network participants and detect hidden services.

```
nmap -sS -sC -sV -p443 -iL hosts -Pn --open
```

This way, an attacker can detect:

- Bootnodes

- Explorer web

Recommendations:

- As long as Explorer is considered, use a separate host with its unique IP address for the Parity client.
- Implement Basic Authentication to restrict access to services.

3.2.3. Information disclosure (3)

Description:

By its design, the Ethereum network enables an attacker to identify network validators.

Impact:

An attacker can use the obtained information to conduct a further attack.

Vulnerable resource:

- poa.network

Technical details:

To identify network validators, it is necessary to establish a connection to all the users in the network. The users with that send new blocks fastest are validators (miners).

Recommendations:

- Use anti-DOS protection for validators.

3.2.4. Information disclosure (4)

Description:

The case for the netstat service detection.

Impact:

An attacker can detect and attack a service to get control over it.

Vulnerable resource:

- red-netstats.poa.network

Technical details:

By exploiting the vulnerability described in the par. 3.2.2, an attacker may disclose the name of the red-explorer.poa.network service and then red-netstats.poa.network as well, as long as the latter has the same semantics.

Recommendations:

Implement Basic Authentication of services for access restriction.

4. DOS testing

4.1. Plan of performed tests

After analyzing the System, ”Digital Security” and its experts developed a detailed testing plan that would emulate possible scenarios of an attack on the System.
Used testing methods:

1. An attack on communication channels and devices.

Creating mass connections to the System and junk traffic to block a communication channel and to complicate the process of counteracting an attack. If successful, this attack may lead to the depletion of OS resources and the resources of network devices used at the point of entry in the OS.

4.2. Testing results

4.2.1. Host 35.167.218.240 (Validator-1)

Testing timeframe: *07.12.2017*

Type: network capacity exhaustion; TCP/UDP flood.

The scope of the testing:
Attack start time: **16:05 (GMT+3)**
The attack was performed with TCP traffic. The traffic was generated with the power of 5 Gbit/s on port 80. The attack was blocked by Amazon service provider. No changes in the System operation were detected.
Attack end time: **16:10 (GMT+3)**

Attack start time: **16:12 (GMT+3)**
The power of the UDP flood attack was increased to 5 Gbit/s. There was a 785 Mb/s load on the channel detected. After that, the host was no longer available.
Attack end time: **16:20 (GMT+3)**

Attack start time: **16:25 (GMT+3)**
It was decided to decrease the power of the attack to 2.5 Gbit/s. There was a 784 Mb/s load on the channel detected, after which the host was no longer available.
Attack end time: **16:30 (GMT+3)**

Attack start time: **16:32 (GMT+3)**
It was decided to decrease the power of the attack to 1.1 Gbit/s. There was a 750 Mb/s load on the channel detected. The host could respond requests. No changes in its operation were noted.

Attack end time: **16:35 (GMT+3)**

Attack start time: **16:40 (GMT+3)**
It was decided to increase the power of the attack to 1.5 Gbit/s. There was a 784 Mb/s load on the channel detected. The host could respond requests. No significant changes in its operation were noted.
Attack end time: **16:42 (GMT+3)**

Attack start time: **16:45 (GMT+3)**
It was decided to increase the power of the attack to 2 Gbit/s. There was a 784 Mb/s load on the channel detected. The host could respond requests. No significant changes in its operation were noted.
Attack end time: **16:50 (GMT+3)**

Attack start time: **16:55 (GMT+3)**
It was decided to increase the power of the attack to 3 Gbit/s. There was a 784 Mb/s load on the channel detected. After that, the host was no longer available.
Attack end time: **17:02 (GMT+3)**

4.2.2. Host 35.166.168.95 (Master of Ceremony)

Testing timeframe: *07.12.2017*

Type: channel capacity exhaustion attack. UDP flood.

The scope of the testing:
Attack start time: **17:20 (GMT+3)**
The attack was performed with UDP traffic. The traffic was generated with the power of 3.5 Gbit/s on port 30303. There was a 784 Mb/s load on the channel detected. Access to the host is restricted.
Attack end time: **17:30 (GMT+3)**

Attack start time: **17:35 (GMT+3)**
It was decided to increase the power of the attack to 7 Gbit/s. Access to the host is hindered. A network operation failure was detected. The host disconnected from other network participants.
Attack end time: **17:43 (GMT+3)**

4.2.3. Host 34.216.117.87 (Bootnode-1)

Testing timeframe: *07.12.2017*

Type: channel capacity exhaustion attack. UDP/TCP flood.

Testing timeframe:

Attack start time: **17:45 (GMT+3)**
The attack was performed with UDP traffic. The traffic was generated with the power of 2.5 Gbit/s on port 30303. No changes in the host operation were detected.
Attack end time: **17:50 (GMT+3)**

Attack start time: **18:00 (GMT+3)**
.
It was decided to increase the power of the attack to 4 Gbit/s. Access to the host is hindered. A network operation failure was detected. The host disconnected from other network participants.
Attack end time: **18:05 (GMT+3)**

Attack start time: **18:10 (GMT+3)**
It was decided to decrease the power of the attack to 2.5 Gbit/s. Server responded requests irregularly.
Attack end time: **18:15 (GMT+3)**

Attack start attack: **18:27 (GMT+3)**
The power was reduced to 1.5 Gbit/s. Server responded requests irregularly.
Attack end time: **18:30 (GMT+3)**

Attack start time: **18:36 (GMT+3)**
The power was reduced to 1 Gbit/s. No changes in the host operation were detected.
Attack end time: **18:38 (GMT+3)**

Attack start time: **18:44 (GMT+3)**
The attack was performed with TCP traffic. The traffic was generated with the power of 1 Gbit/s on port 443. No changes in the host operation were detected.
Attack end time: **18:46 (GMT+3)**

Attack start time: **18:50 (GMT+3)**
The power was increased to 1.5 Gbit/s. No changes in the host operation were detected.
Attack end time: **18:55 (GMT+3)**

Attack start time: **18:58 (GMT+3)**
The power of attack was increased to 3 Gbit/s. No changes in the host operation were detected.
Attack end time: **19:01 (GMT+3)**

Attack start time: **19:05 (GMT+3)**

The power of attack was increased to 8 Gbit/s. The server stopped responding requests. There were failures detected in the network operation.
Attack end time: **19:10 (GMT+3)**

4.2.4. Hosts 34.216.117.87 (Bootnode-1), 34.208.23.103 (Bootnode-2)

Testing timeframe: *07.12.2017*

Type: Channel capacity exhaustion attack. UDP/TCP flood.

The scope of the testing:
Attack start time: **19:17 (GMT+3)**
The attack was performed with UDP traffic. The traffic was generated with the power of 8 Gbit/s on port 30303 on both hosts in the scope. Both hosts stopped responding requests
Attack end time: **19:20 (GMT+3)**

4.2.5. Host red.poa.network (balancer)

Testing timeframe: *07.12.2017*

Type: Channel capacity exhaustion attack. TCP flood.

The scope of the testing:
Attack start time: **19:17 (GMT+3)**
The attack was performed with TCP traffic. The traffic was generated with the power of 5 Gbit/s on port 443 on both hosts in the scope. The CDN managed to counteract malicious traffic. No changes in the host operation were detected.
Attack end time: **19:28 (GMT+3)**

5. Conclusion

In the scope of the security assessment, “Digital Security” experts detected the vulnerabilities of “high” and “average” impact levels, as well as the security issues that may lead to the disclosure of the information stored in the System. These vulnerabilities and security weaknesses can be used by an attacker to compromise the Netstat and Explorer hosts.

As a result of stress testing of the System, the experts have managed to determine the power levels of traffic required to disrupt different network nodes.

The overall security level of the System was rated “Medium.”

Appendix 1. Security level analysis. Background information.

Security level analysis

To analyze the System security level, it is necessary to measure severity and likelihood of the detected vulnerabilities exploitation. The likelihood of exploitation is measured, according to the ease of vulnerability exploitation and the accessibility of a vulnerability.

Vulnerability severity

The “Severity” property of a vulnerability describes possible results of this vulnerability exploitation, regarding confidentiality, integrity, and availability of information processed on a vulnerable resource. Severity levels are described in the Table A-1.

Table A–1. Severity levels

Severity level	Confidentiality violation	Integrity violation	Availability violation
None	Does not happen.	Does not happen.	Does not happen.
Low	Obtaining access to a noncritical information by an attacker through privilege escalation	Integrity violation of a noncritical information by an attacker with basic user rights in the System	Short-time denial-of-service of a mission-critical application
Medium	Confidentiality violation of sensitive data by an attacker with basic user rights in the System	Integrity violation of sensitive data by an attacker with basic user rights in the System	Denial of service of a mission-critical application or a short-time denial of service of the System
High	Confidentiality violation of critical information by an attacker with administrator rights in the System	Integrity violation of critical information by an attacker with administrator rights in the System	Denial of Service of the System

Ease of vulnerability exploitation

The “Ease of exploitation” property of a vulnerability defines what hardware and software, time and computing resources, and professional skills are required to exploit a vulnerability (Table A-2).

Table A–2. Ease of vulnerability exploitation levels

Level	Description
Low	Vulnerability exploitation requires high computing powers, significant time resources, developing new software, configuration analysis of the System, determination and testing possible ways and conditions of successful exploitation of this vulnerability.
Medium	Vulnerability exploitation requires high-performance computing, extensive time resources, special hardware and software, and analysis of a violated system configuration. An attacker does not have to have deep knowledge of the system or professional skills to perform an attack.
High	Vulnerability exploitation does not require the use of any special hardware or software, high-performance computing, time resources or any professional skills to perform an attack.

Vulnerability availability

The “Accessibility” property of a vulnerability defines what user classes have access to a vulnerable resource (Table A-3).

Table A–3. Accessibility levels

Level	Description
Low	Privileged users
Medium	Registered users
High	All users

Likelihood of exploitation

The likelihood of exploitation is calculated according to “ease of exploitation” and “accessibility” levels (Table A–4).

Table–4. Likelihood of exploitation

Likelihood of exploitation		Ease of exploitation		
		Low	Medium	High
Accessibility	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Vulnerability impact

Vulnerability impact (for one of the existing threats) is measured, according to vulnerability severity (for one of the existing threats) and the likelihood of exploitation of a vulnerability (Table A-5).

Table A–5. Vulnerability impact levels

Vulnerability impact		Likelihood of exploitation		
		Low	Medium	High
Vulnerability severity	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Appendix 2. The list of vulnerabilities and security weaknesses detected in the System.

The vulnerabilities and security weaknesses detected in the System are listed in Table B-1.

Table B-1. The list of the detected vulnerabilities and security weaknesses

External audit of the System		
Vulnerability	Overall impact level	See paragraph
Denial of Service	High	3.1.3.
Outdated server software	Medium	3.1.1.
Debugging information read-out	Low	3.1.2.
Security weakness		See paragraph
Information disclosure (1)		3.2.1.
Information disclosure (2)		3.2.2.
Information disclosure (3)		3.2.3.
Information disclosure (4)		3.2.4.