Digital Security

БЕЗОПАСНОСТЬ КАК ИСКУССТВО

КОНФИДЕНЦИАЛЬНО

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

по результатам проведения
анализа защищённости и нагрузочного тестирования
сети PoA.Network

Даты проведения работ:
7.12.17- 13.12.17
Технический менеджер проекта:
А.О. Перцев
Директор департамента аудита:
А.Н. Тюрин

1. Введение

1.1. Общие положения

В настоящем экспертном заключении представлены результаты проведения работ по анализу защищенности и нагрузочному тестированию сети Proof-of-Authority (далее - Система), принадлежащей PoA.Network (далее – Компания), а также предложены рекомендации по устранению выявленных уязвимостей и повышению уровня защищенности.

1.2. Принятые сокращения

Таблица 1.2–1. Принятые сокращения

Сокращение	Расшифровка
ИБ	Информационная безопасность
ИС	Информационная система
ПО	Программное обеспечение
PoA	Proof-of-Authority
DOS	Deny of Service

1.3. Резюме

В соответствии с договором № ДСС-КУ-2017/38 от 04.12.2017г. специалистами компании «Digital Security» в период с 07.12.17 по 13.12.17 были проведены работы по анализу защищенности и нагрузочному тестированию Системы.

Была рассмотрена модель внешнего нарушителя.

Проведенные работы показали, что, используя слабость п. 3.2.3., внешний атакующий может установить реальные IP-адреса всех валидаторов (майнеров) и вывести сеть из строя с помощью DOS атаки мощностью 3 Гбит/с (п. 4.2.1.).

Основными рекомендациями являются:

1. Устранение выявленных технических уязвимостей;
2. Устранение выявленных архитектурных уязвимостей.

Далее содержатся подробности описания выявленных недостатков и связанных с ними рисков информационной безопасности, а также детальные рекомендации по устранению уязвимостей.

1.4. Область аудита

В область проведения работ вошел перечень хостов Компании, представленный в Таблице 1.4.

Таблица 1.4. Перечень хостов Компании для анализа защищённости

№ п/п	IP-адрес	Функция/Назначение/Название
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 (балансировщик)

2. Принципы проведения работ

2.1. Угрозы ИБ

На информационные ресурсы Компании могут действовать следующие три угрозы ИБ: угрозы нарушения конфиденциальности, целостности и доступности.

Угроза нарушения конфиденциальности направлена на разглашение информации, имеющей в Компании статус конфиденциальной. При реализации угрозы информация становится известной лицам, которые не должны иметь к ней доступ – ряду сотрудников Компании, клиентам, партнерам, конкурентам, третьим лицам.

Угроза нарушения целостности направлена на модификацию или искажение информации, приводящее к изменению ее структуры или смысла, полному или частичному уничтожению.

Угроза нарушения доступности (угроза отказа в обслуживании) заключается в невозможности получения доступа к информационному ресурсу пользователями информационной системы.

Основным принципом проведения аудита ИБ является проверка возможности реализации указанных угроз, воздействующих на информационные ресурсы Системы, в рамках заданной модели нарушителя.

2.2. Модель нарушителя

В качестве вероятного нарушителя информационной безопасности Системы Компании рассматривается лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий потенциально могут реализовать угрозы ИБ, осуществить посягательства на информационные ресурсы Системы и нанести ущерб интересам Компании.

В качестве угроз ИБ рассматриваются базовые угрозы нарушения конфиденциальности и целостности информации, а также угроза отказа Системы в обслуживании клиентов Компании.

Умышленно действующий нарушитель может преследовать следующие цели (а также их всевозможные комбинации):

- злонамеренный вызов отказа в обслуживании;
- повышение собственных привилегий;
- несанкционированный доступ к критичной с точки зрения бизнеса информации.

В ходе работы была использована модель внешнего нарушителя.

2.2.1. Внешний нарушитель

При проведении анализа защищенности используются следующие модели внешнего нарушителя:

- внешний нарушитель из сети Интернет, обладающий знаниями о тестируемой Системе из публичных источников, но не обладающий правами в ней.

3. Внешний анализ Системы

3.1. Перечень обнаруженных уязвимостей

3.1.1. Устаревшая версия серверного ПО

Критичность: *средняя*
Вероятность эксплуатации: *средняя*
Итоговый риск: *средний*

Описание:

В качестве компонента Системы используется ПО устаревшей версии, которая имеет множество общеизвестных уязвимостей.

Риск:

Злоумышленник может проводить различные успешные атаки на веб-сервер и другое ПО, для которого отсутствуют обновления. Последствия могут быть различны, в зависимости от типа уязвимости.

Уязвимые ресурсы:

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

Технические детали:

Публично доступные packages.json приложений chain-explorer и eth-netstats свидетельствуют об использовании компонентов (модулей) устаревших версий, многие их которых имеют критичные уязвимости.
Источники package.json:

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

Рекомендации:

- Обновить программное обеспечение до актуальных версий;
- Внедрить процесс систематического обновления серверного ПО.

3.1.2. Вывод отладочной информации

Критичность: низкая
Вероятность эксплуатации: средняя
Итоговый риск: низкий

Описание:

В Системе разрешен вывод отладочной информации в случае сбоев в работе.

Риск:

По ответам от сервера злоумышленник имеет возможность выяснить версию ПО, используемые классы, пути установки веб-приложения и использовать данную информацию в будущем для проведения целенаправленных атак.

Уязвимый ресурс:

- red-netstats.poa.network

Технические детали:

По умолчанию expressjs версии 4.13.3 пытается обработать тело HTTP-запроса вне зависимости от HTTP method'a. В данном примере expressjs пытается обработать тело запроса как json, что приводит к ошибке, поскольку оно пустое.
Пример запроса:

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

Пример ответа:

```
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>
```

Рекомендации:

- Отключить вывод отладочной информации;
- Обновить Expressjs-сервер.

3.1.3. Отказ в обслуживании

Критичность: средняя
Вероятность эксплуатации: высокая
Итоговый риск: высокий

Описание:

Потенциальный злоумышленник может вызвать отказ в обслуживании сервиса.

Риск:

Отказ в обслуживании сервиса Explorer может привести к тому, что обычные пользователи не смогут получать информацию о состоянии аккаунтов и транзакциях в сети.

Уязвимый ресурс:

- red-explorer.poa.network

Технические детали:

Все запросы, в ходе которых так или иначе происходит получение информации из blockchain, могут быть использованы для проведения атаки «отказ в обслуживании». В качестве примера приведен запрос на получение данных от транзакции.
Пример запроса:

```
GET /tx/<ПРОИЗВОЛЬНЫЙ ХЕШ>
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
```

Если повторять запрос с одного хоста в 30 и более потоков, сервис становится недоступен для всех пользователей.

Рекомендации:

- Внедрить механизм CAPTCHA для «долгих» запросов.

3.2. Перечень обнаруженных слабостей

3.2.1. Раскрытие информации (1)

Описание:

Любой участник сети может узнать реальные IP-адреса участников сети.

Риск:

Злоумышленник может использовать полученную информацию для дальнейших атак.

Уязвимый ресурс:

- poa.network

Технические детали:

Получить все IP-адреса можно с помощью следующей команды:

```
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. Раскрытие информации (2)

Описание:

Parity-клиент развернут на том же хосте, что и веб-сервис, что позволяет обнаружить его (веб-сервис) в сети.

Риск:

Злоумышленник может установить IP-адреса веб-ресурсов в сети (Explorer web) и атаковать их.

Уязвимый ресурс:

- red-explorer.poa.network

Технические детали:

Получив список IP-адресов всех участников в сети, атакующий может просканировать его на предмет дополнительных открытых портов и, таким образом, имперсонировать участников сети и найти скрытые сервисы.

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

Таким образом могут быть обнаружены:

- Bootnodes
- Explorer web

Рекомендации:

- Для сервиса Explorer вынести Parity-клиент на отдельный хост с другим IP-адресом.
- Внедрить Basic Authentication для служебных сервисов для ограничения доступа.

3.2.3. Раскрытие информации (3)

Описание:

Сеть Ethereum, исходя из своего дизайна, позволяет определять валидаторов в сети.

Риск:

Злоумышленник может использовать эти знания для дальнейшей атаки.

Уязвимый ресурс:

- poa.network

Технические детали:

Для установления валидатора в сети необходимо установить соединение со всеми участниками в сети, и те участники, от которых быстрее всего будут приходить новые блоки, будут являться валидаторами (майнерами).

Рекомендации:

- Вести учет и контроль участников в сети.

3.2.4. Раскрытие информации (4)

Описание:

Сценарий обнаружения сервиса netstat.

Риск:

Злоумышленник может обнаружить и атаковать служебный сервис получения контроля над ним.

Уязвимый ресурс:

- red-netstats.poa.network

Технические детали:

Используя 3.2.2, атакующий может установить доменное имя сервиса red-explorer.poa.network и далее, используя семантику этого названия, подобрать доменное имя red-netstats.poa.network.

Рекомендации:

- Внедрить Basic Authentication для служебных сервисов для ограничения доступа.

4. Тестирование на отказ в обслуживании

4.1. Фактический план работ

Компанией и специалистами Digital Security после анализа Системы был разработан план проведения тестирования, который соответствовал бы возможным вариантам атак на Систему.

Использованные методы тестирования:

1. Атака на каналы связи и оборудование

Генерация массовых подключений к Системе и «мусорного» трафика для забивания канала связи и затруднения блокировки атаки. Это потенциально может привести к исчерпанию доступных ресурсов ОС, а также сетевого оборудования, расположенного на подходе к ОС.

4.2. Результаты тестирования

4.2.1. Хост 35.167.218.240 (Validator-1)

Дата проведения тестирования: *07.12.2017*

Тип: атака на израсходование пропускной способности канала. TCP/UDP flood.

Ход проведения тестирования:

Время начала атаки: **16:05 (GMT+3)**

Атака осуществлялась TCP-трафиком. TCP трафик генерировался на уровне 5 Гбит/с на 80 порт. Атака была заблокирована средствами провайдера Amazon. Существенных изменений в работе Системы выявлено не было.

Время окончания атаки: **16:10 (GMT+3)**

Время начала атаки: **16:12 (GMT+3)**

Далее была увеличена мощность UDP flood-атаки до 5 Гбит/с. На сервере была зафиксирована нагрузка на канал в 784 Мб/с, после чего хост перестал быть доступен.

Время окончания атаки: **16:20 (GMT+3)**

Время начала атаки: **16:25 (GMT+3)**

Было принято решение уменьшить мощность атаки до 2.5 Гбит/с. На сервере была зафиксирована нагрузка на канал в 784 Мб/с, после чего хост перестал быть доступен.

Время окончания атаки: **16:30 (GMT+3)**

Время начала атаки: **16:32 (GMT+3)**

Было принято решение уменьшить мощность атаки до 1.1 Гбит/с. На сервере была зафиксирована нагрузка на канал в 750 Мб/с. Хост отвечает на запросы, существенных изменений в его работе не зафиксировано.

Время окончания атаки: **16:35 (GMT+3)**

Время начала атаки: **16:40 (GMT+3)**

Было принято решение увеличить мощность атаки до 1.5 Гбит/с. На сервере была зафиксирована нагрузка на канал в 784 Мб/с. Хост отвечает на запросы, существенных изменений в его работе не зафиксировано.

Время окончания атаки: **16:42 (GMT+3)**

Время начала атаки: **16:45 (GMT+3)**

Было принято решение увеличить мощность атаки до 2 Гбит/с. На сервере была зафиксирована нагрузка на канал в 784 Мб/с. Хост отвечает на запросы, существенных изменений в его работе не зафиксировано.

Время окончания атаки: **16:50 (GMT+3)**

Время начала атаки: **16:55 (GMT+3)**

Было принято решение увеличить мощность атаки до 3 Гбит/с. На сервере была зафиксирована нагрузка на канал в 784 Мб/с, после чего хост перестал быть доступен.

Время окончания атаки: **17:02 (GMT+3)**

4.2.2. Хост 35.166.168.95 (Master of Ceremony)

Дата проведения тестирования: *07.12.2017*

Тип: атака на израсходование пропускной способности канала. UDP flood.

Ход проведения тестирования:

Время начала атаки: **17:20 (GMT+3)**

Атака осуществлялась UDP-трафиком. UDP-трафик генерировался на уровне 3.5 Гбит/с на 30303 порт. На сервере была зафиксирована нагрузка на канал в 784 Мб/с, доступ к хосту затруднен.

Время окончания атаки: **17:30 (GMT+3)**

Время начала атаки: **17:35 (GMT+3)**

Было принято решение увеличить мощность атаки до 7 Гбит/с. Доступ к хосту затруднен. Зафиксирован сбой в работе сети. Хост отключился от других участников сети.

Время окончания атаки: **17:43 (GMT+3)**

4.2.3. Хост 34.216.117.87 (Bootnode-1)

Дата проведения тестирования: *07.12.2017*

Тип: атака на израсходование пропускной способности канала. UDP/TCP flood.

Ход проведения тестирования:

Время начала атаки: **17:45 (GMT+3)**

Атака осуществлялась UDP-трафиком. UDP-трафик генерировался на уровне 2.5 Гбит/с на 30303 порт. Изменений в работе хоста зафиксировано не было

Время окончания атаки: **17:50 (GMT+3)**

Время начала атаки: **18:00 (GMT+3)**

Было принято решение увеличить мощность атаки до 4 Гбит/с. Доступ к хосту затруднен. Зафиксирован сбой в работе сети. Хост отключился от других участников сети.

Время окончания атаки: **18:05 (GMT+3)**

Время начала атаки: **18:10 (GMT+3)**

Было принято решение уменьшить мощность атаки до 2.5 Гбит/с. Сервер нестабильно отвечает на запросы.

Время окончания атаки: **18:15 (GMT+3)**

Время начала атаки: **18:27 (GMT+3)**

Мощность атаки уменьшена до 1.5 Гбит/с. Сервер нестабильно отвечает на запросы.
Время окончания атаки: **18:30 (GMT+3)**

Время начала атаки: **18:36 (GMT+3)**
Мощность атаки уменьшена до 1 Гбит/с. Изменений в работе сервера замечено не было.
Время окончания атаки: **18:38 (GMT+3)**

Время начала атаки: **18:44 (GMT+3)**
Атака осуществлялась TCP-трафиком. TCP-трафик генерировался на уровне 1 Гбит/с на 443 порт. Изменений в работе хоста зафиксировано не было
Время окончания атаки: **18:46 (GMT+3)**

Время начала атаки: **18:50 (GMT+3)**
Мощность атаки увеличена до 1.5 Гбит/с. Изменений в работе сервера замечено не было.
Время окончания атаки: **18:55 (GMT+3)**

Время начала атаки: **18:58 (GMT+3)**
Мощность атаки увеличена до 3 Гбит/с. Изменений в работе сервера замечено не было.
Время окончания атаки: **19:01 (GMT+3)**

Время начала атаки: **19:05 (GMT+3)**
Мощность атаки увеличена до 8 Гбит/с. Сервер перестал отвечать на запросы. В сети обнаружены сбои.
Время окончания атаки: **19:10 (GMT+3)**

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

Дата проведения тестирования: *07.12.2017*

Тип: Атака на израсходование пропускной способности канала. UDP/TCP flood.

Ход проведения тестирования:
Время начала атаки: **19:17 (GMT+3)**
Атака осуществлялась UDP-трафиком. UDP-трафик генерировался на уровне 8 Гбит/с на 30303 порт на каждый из хостов. Оба хоста перестали отвечать запросы.
Время окончания атаки: **19:20 (GMT+3)**

4.2.5. Хост red.poa.network (балансировщик)

Дата проведения тестирования: *07.12.2017*

Тип: атака на израсходование пропускной способности канала. TCP flood.

Ход проведения тестирования:

Время начала атаки: **19:17 (GMT+3)**

Атака осуществлялась TCP-трафиком. TCP-трафик генерировался на уровне 5 Гбит/с на 443 порт на каждый из хостов. CDN успешно справился с паразитным трафиком. Изменений в работе хостов замечено не было.

Время окончания атаки: **19:28 (GMT+3)**

5. Заключение

В результате анализа защищенности Системы специалистами Digital Security были выявлены уязвимости низкого, среднего и высокого уровня критичности. Кроме того, были выявлены слабости, приводящие к раскрытию информации о Системе, которые злоумышленник может использовать для других атак с целью компрометации хостов Netstat и Explorer.

В результате нагрузочного тестирования Системы были определены мощности, необходимые для выведения из строя различных узлов в сети.

Общий уровень защищенности Системы можно охарактеризовать как «средний».

Приложение 1. Анализ уровня защищенности. Справочная информация.

Анализ уровня защищенности

Для анализа уровня защищенности необходимо оценить критичность и вероятность реализации выявленных в ходе аудита уязвимостей. Вероятность реализации определяется доступностью и простотой реализации уязвимости.

Критичность реализации уязвимости

Свойство «критичность реализации» некоторой уязвимости характеризует возможные последствия реализации данной уязвимости с точки зрения угроз нарушения конфиденциальности, целостности и доступности информации, обрабатываемой на уязвимом ресурсе. Описание уровней критичности реализации уязвимостей приведено в Таблице А–1.

Таблица А–1. Уровни критичности уязвимостей

Значение	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Отсутствует	Не происходит	Не происходит	Не происходит
Низкий	Получение нарушителем доступа к некритичной информации в результате эскалации привилегий	Нарушение целостности некритичной информации с правами обычного пользователя	Кратковременный отказ в обслуживании критичного приложения
Средний	Нарушение конфиденциальности критичной информации с правами обычного пользователя	Нарушение целостности критичной информации с правами обычного пользователя	Отказ в обслуживании критичного приложения или кратковременный отказ в обслуживании
Высокий	Нарушение конфиденциальности критичной информации с	Нарушение целостности критичной информации с	Отказ в обслуживании

	правами администратора	правами администратора	

Простота эксплуатации уязвимости

Свойство «простота эксплуатации» некоторой уязвимости определяет, какие аппаратные и программные средства, профессиональные навыки, а также какое количество временных и вычислительных ресурсов, необходимо потенциальному нарушителю для реализации некоторой уязвимости (Таблица А–2).

Таблица А–2. Уровни простоты эксплуатации уязвимости

Значение	Описание
Низкий	Для эксплуатации уязвимости требуется разработка новых программных средств, проведение анализа конфигурации атакуемой системы, выявление и проверка различных возможных путей и условий успешной эксплуатации данной уязвимости, вычислительные мощности или временной резерв. Атакующий должен обладать значительными профессиональными навыками и познаниями в специфичных областях.
Средний	Для эксплуатации уязвимости требуется наличие специальных программных или аппаратных средств, проведение анализа конфигурации атакуемой системы, вычислительные мощности или временной резерв. Атакующему достаточно обладать незначительным объемом профессиональных навыков и познаний для реализации атаки.
Высокий	Для эксплуатации уязвимости не требуется использование специальных аппаратных или программных средств, значительные вычислительные мощности или временной резерв, детальное знание конфигурации атакуемой системы. Атакующему для реализации атаки не требуются специфичные профессиональные навыки и познания.

Доступность уязвимости

Свойство «доступность» некоторой уязвимости определяет, каким классам пользователей доступен уязвимый ресурс (Таблица А–3).

Таблица А–3. Уровни доступности

Значение	Описание
Низкий	Привилегированные пользователи
Средний	Зарегистрированные пользователи
Высокий	Все пользователи

Вероятность эксплуатации уязвимости

Вероятность эксплуатации уязвимости рассчитывается на основе простоты эксплуатации и области доступности уязвимости по таблице А–4.

Таблица А–4. Уровень вероятности эксплуатации

Вероятность эксплуатации		Простота эксплуатации		
		Низкий	Средний	Высокий
Доступность	Низкий	Низкий	Низкий	Средний
	Средний	Низкий	Средний	Высокий
	Высокий	Средний	Высокий	Высокий

Риск уязвимости

Риск уязвимости (по одной из угроз) рассчитывается на основе критичности уязвимости (по одной из угроз) и вероятности эксплуатации уязвимости по таблице А–5.

Таблица А–5. Уровень риска

Риск уязвимости		Вероятность эксплуатации		
		Низкий	Средний	Высокий
Критичность уязвимости	Низкий	Низкий	Низкий	Средний
	Средний	Низкий	Средний	Высокий
	Высокий	Средний	Высокий	Высокий

Приложение 2. Перечень обнаруженных уязвимостей и слабостей Системы. Справочная информация.

Обнаруженные в ходе работ уязвимости и слабости Системы представлены в таблице Б-1.

Таблица Б-1. Перечень обнаруженных уязвимостей и слабостей Системы

Внешний аудит Системы		
Уязвимость	**Итоговый риск**	**Подробности в пункте**
Отказ в обслуживании	Высокий	3.1.3.
Устаревшая версия серверного ПО	Средний	3.1.1.
Вывод отладочной информации	Низкий	3.1.2.
Слабость		**Подробности в пункте**
Раскрытие информации (1)		3.2.1.
Раскрытие информации (2)		3.2.2.
Раскрытие информации (3)		3.2.3.
Раскрытие информации (4)		3.2.4.