Сентябрь 2022

Аудит безопасности

Tetherex

TVrHddERScoUvfgAViceSQz83weZpsyjdE

https://grox.solutions

Критические ошибки (критическая, высокая опасность): **0**

Ошибки и уязвимости, которые могут вести к потере, краже или намеренному выводу средств на адреса третьих лиц (бэкдоры). Недопустимые ошибки и баги для деплоя на основную сеть. Важные предупреждения для владельцев, клиентов или инвесторов проекта.

Проблемы, баги и предупреждения (средняя, низкая опасность): **0**

Баги и ошибки, возможности нарушения запланированной структуры, функционала или логики смарт-контракта. Отсутствие необходимых предосторожностей в коде. Прочие предупреждения.

Возможности оптимизации (очень низкая опасность): **2**

Возможности снизить стоимость транзакций при использовании смарт-контракта или уменьшить размер хранимых данных в блокчейне.

Примечания и рекомендации (очень низкая опасность): **2**

Прочие заметки, рекомендации и предложения, а также проблемы, не влияющие на функционал смарт-контракта.

Заключение:

В контракте Tetherex не было обнаружено критических замечаний (уязвимостей или бэкдоров). Код был построчно проаудирован на предмет всех известных и возможных проблем.

Смарт-контракт соответствует всем стандартам и безопасен для использования в основной сети.

Предупреждение: не отправляйте токены на адрес смарт-контракта обычным трансфером. Чтобы создать депозит необходимо «одобрить» (approve function) необходимую сумму токенов в контракте USDT TRC20 Token, затем вызвать функцию invest в Tetherex.

Результаты аудита:

Возможности оптимизации

1. Запись статистических параметров в блокчейн:

Список статистических параметров, запись в которые повышают стоимость транзакций и увеличиваем объем данных хранящихся в блокчейне:

```
uint256 public totalUsers;
uint256 public totalInvested;
uint256 public totalWithdrawn;
uint256 public totalDeposits;
uint256 public totalIncomes;
```

Рекомендация: используйте ивенты и логгируйте данную информацию вместо записи в блокчейн.

Примечание: данный пункт не влияет на функционал смарт-контракта.

2. Рассылка реферальных бонусов:

В контракте реализована 3-уровневая реферальная система и все выплаты происодят внутри транзакции инвестиции. Данное действие (до 3 дополнительных отправок) повышает стоимость транзакции.

Рекомендация: использовать начисление бонусов к выводу (при котором каждый пользователь сам запрашивает свои средства) вместо прямой отправки.

Примечания

3. Циклы по параллельным депозитам (очень низкая опасность):

В функциях withdraw, getUserDividends, getUserAvailable, getUserTotalDeposits, getUserTotalWithdrawn циклы неограниченно растут при увеличении количества депозитов. При создании большого количества параллельных депозитов с одного кошелька это может привести к чрезмерному повышению стоимости транзакции и невозможности вывести дивиденды ввиду лимита размера транзакции в сети.

4. Закрытие последней выплаты (очень низкая опасность).

В случае если у последнего покидающего проект пользователя выплата будет больше чем баланс смарт-контракта – он получит весь доступный остаток на балансе, но при этом будет зафиксировано, что была закрыта вся выплата.

Примечание: данный комментарий не критичен, так как после опустошения баланса смарт-контракта маловероятно что контракт будет использоваться вновь. Поэтому последнему пользователю выгодно получить хоть какую-либо сумму.

Независимое описание функционала смарт-контракта:

Контракт Tetherex обеспечивает пользователю возможность инвестировать любую сумму в TRC20 токенах USDT (от 50 USDT включительно) в контракт и получить 200% возврат инвестиций, в случае если на балансе контракта будет достаточно средств для выплаты.

Дивиденды выплачиваются из депозитов пользователей (схема Понци).

Примечание: USDT TRC20 Token смарт-контракт - https://tronscan.org/#/contract/TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t

Предупреждение: не отправляйте токены на адрес смарт-контракта обычным трансфером. В этом случае вы потеряете свои токены.

Чтобы создать депозит необходимо использовать двухшаговую отправку токенов:

1) Вызов “approve” функции внутри USDT Token.
2) Вызов “invest” функции внутри Tetherex. Минимальная сумма - 50 USDT.

Данный процесс обусловлен общеизвестной проблемой стандарта ERC20 «отсутствие механизма обработки транзакций». Подробнее читайте в нашей статье: https://grox.solutions/ru/all/erc20-issues

Каждый последующий вклад ведется раздельно в контракте, с целью сохранения суммы выплаты по каждому депозиту.

Начисляемый пользователю суточный процент начинается от 3% и зависит от следующих факторов:

- За каждые 20 000 USDT на балансе смарт-контракта +0.1% до 23% (процент не снижается при падении баланса).

- За каждые 12 часов невывода дивидендов со смарт-контракта +0.1% (при создании повторных депозитов счетчик не сбивается).

Максимальный суточный процент не ограничен (3+20+HoldBonus).

Трех-уровневая реферальная программа: в функции invest можно указать адрес реферера.

В результате пригласитель получит прямым трансфером долю депозита приглашенного пользователя в соответствии со следующими условиями:

Уровень реферала	1	2	3
Процент, %	6	2	1

Требования к указываемому рефереру: рефером нельзя указать собственный кошелек, а также кошелек не имеющий хотя бы одного вклада в смарт-контракте.

Реферер указывается одноразово в момент любого вклада и закрепляется за пользователем без возможности изменения. С каждого последующего вклада процент также будет начисляться рефереру.

Комиссия владельцев контракта 11%, часть средств отправляется на 3 адреса:

(marketing address) - 5%.
(platform address) - 5%.
(admin address) - 1%.

В контракте присутствуют статистические функции не требующие отправки транзакций:

1. `getContractBalance` – баланс контракта в USDT (6 знаков после запятой).

2. `getContractBalanceRate` - текущий процент контракта (1 знак после запятой, 30=3%).

3. `getUserReferrer` – реферер пользователя (пригласитель).

4. `getUserAvailable` – доступные дивиденды к выводу.

5. `isActive` – есть ли у пользователя активные депозиты.

6. `getUserAmountOfDeposits` – количество депозитов пользователя.

7. `getUserTotalDeposits` – сумма вложенных средств пользователем.

8. `getUserTotalWithdrawn` – сумма выведенных средств пользователем.

9. `getUserReferralBonus` - сумма рефбонусов юзера всех 3 уровней.

10. `getUserDepositInfo` - данные о депозита (по индексу): сумма депозита, сумма выведенных средств, UNIX дата старта депозита.

Сентябрь 2022

Дисклеймер:

Данный аудит не является призывом к участию в проекте и относится только к коду указанного смарт-контракта.

Не забывайте что вы совершаете все действия связанные с финансами только на свой страх и риск, особенно если вы участвуете в высокорисковых проектах.

Предупреждение:

Остерегайтесь поддельных аудитов и мошенников.
Вся официальная информация находится на 3 ресурсах:

Website: **www.grox.solutions**
Telegram: **www.t.me/grox_solutions (@grox_solutions)**
YouTube: **www.youtube.com/c/groxsolutions**

Если у вас остались вопросы по разработке или аудиту смарт-контракта, пожалуйста свяжитесь с нами и мы проконсультируем вас по всем моментам.

Telegram: **www.t.me/gafagilm (@gafagilm)**
E-mail: **info@grox.solutions**