Январь 2021

Аудит безопасности

TRONexVIP

TYfy6fjzRbyNUxna9eiPbjkFE9P275UEuZ

www.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.

Conclusion:

В контракте TRONexVIP 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.

Примечание: данный проект является единственным продолжением оригинального проекта TRONex, остерегайтесь копий.

Результаты аудита:

Возможности оптимизации

1. Запись статистических параметров в блокчейн (очень низкая опасность):

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

```
uint public totalDeposits;
uint public totalInvested;
uint public totalWithdrawn;
uint64 refback;
uint64 bonus;
uint24[5] refs;
```

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

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

2. Рассылка реферальных бонусов (очень низкая опасность):

В контракте реализована 5-уровневая реферальная система и все выплаты происодят внутри транзакции инвестиции. Данное действие (до 6 дополнительных отправок) существенно 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 некорректным отображению и обработке информации.

Примечание: максимум возможного количества депозитов с одного кошелька в контракте - 100.

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 TRONexVIP обеспечивает пользователю возможность инвестировать любую сумму в TRX (от 100 TRX 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).

В проекте не разрешено участвовать со смарт-контракта, только с обыкновенного кошелька.

Создать депозит можно вызвав функцию invest, приложив к транзакции необходимое количество TRX (от 100 TRX включительно).

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

Начисляемый пользователю суточный процент начинается от 1% и зависит от следующих факторов:

- За каждые 250 000 TRX на балансе смарт-контракта +0.05% до 15% (процент не снижается при падении баланса).
- За каждые 12 часов невывода дивидендов со смарт-контракта +0.2% до 15% (37.5 дней). При создании повторных депозитов счетчик не сбивается.
- Бонус за сумму депозитов - каждые 5000 TRX +0.1% (до 750 000 TRX).

Максимальный суточный процент: 50% (5+15+15+15).

Сумма доступных дивидендов рассчитывается в момент запроса и доступна к выводу в любое время.

Вывод пользователем осуществляется вызовом функции withdraw с адреса, с которого был сделан депозит.

Комиссия владельцев контракта: часть вложенных средств отправляется на два адреса:

(marketing address) - 5%.
(fund address) - 5%.

5-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	4-5
Процент, %	5	2	1	0.5

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.

Каждый пользователь имеющий хотя бы один вклад в контракте может установить собственный ‘refBackPercent’ - процент (доля от реферального бонуса) который будет автоматически возвращаться рефералу 1 уровня (приглашенному).

Для того чтобы установить refBackPercent необходимо вызвать функцию ‘setRefBackPercent’ указав процент с двумя знаками после запятой к примеру 1% = 100, 100% = 10000).

В контракте присутствуют статистические функции не требующие отправки транзакций:

1. `getContractBalance` – баланс смарт-контракта.
2. `getUserPercentRate` – процент пользователя (с двумя знаками после запятой).
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. `getUserDeposits` - информация о депозитах пользователя.
10. `getSiteStats` - сумма инвестиций, кол-во депозитов, баланс контракта, текущий бонус контракта.
11. `getUserStats` - процент пользователя, доступные дивиденды, сумма инвестированных средств, количество депозитов и выведенные средства.
12. `getUserReferralStats` - реферер пользователя, процент рефбэка пользователя, процент рефбека реферера и количества депозитов рефералов всех уровней.

Январь 2021

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/groxsolutions (@groxsolutions)**
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**