Аудит контракта TRONexWorld

Редакция 3 от 28.10.2020

Оглавление

Аудит контракта TRONexWorld 1
Краткая информация 3
Сведения 3
Общее заключение 3
Отказ от ответственности 3
Обобщенные данные 4
Полученные данные 4
A. Ошибки 4
B. Замечания 4
C. Улучшения 4
Приложение. Классификация ошибок 5
Приложение. Цифровой отпечаток байткода 6
Приложение. Подпись заключения аудита 7

Краткая информация

Проект: tronex.world
Сеть: TRON
Версия компилятора: 0.5.10+commit.a1d534e
Оптимизация: включена
Дата аудита: 28.10.2020

Сведения

Проведён **повторный** обзор и анализ кода контракта на предмет уязвимостей, логических ошибок и возможности экзит-скама разработчиков. Данная работа была проведена в отношении исходного кода проекта, предоставленного заказчиком.

В процессе аудита не было обнаружено ошибок и замечаний.

Общее заключение

В результате проведенного аудита не было выявлено замечаний, влияющих на безопасность средств пользователей, находящихся на контракте. Явные признаки экзит-скама – не обнаружены. *(экзит скам - ситуация, при которой разработчики контракта имеют контролируемый доступ к средствам участников и могут без их ведома совершать операции вывода)*. Ошибок, брешей в безопасности так же не обнаружено.

Telescr.in гарантирует безопасность и работоспособность контракта TRONexWorld.

Отказ от ответственности

Команда telescr.in в рамках данного аудита не несет ответственности за действия разработчиков или третьих лиц на связанных с данным проектом платформах (сайтах, мобильных приложениях и так далее). Аудит подтверждает и гарантирует лишь правильное функционирование смарт-контракта в редакции, представленной разработчиками проекта (проверить редакцию).

Подтверждено цифровой подписью

Обобщенные данные

Анализ контракта был произведен с помощью следующих методов:

- Статический анализ
  - Проверка кода на типичные ошибки, приводящие к наиболее распространённым уязвимостям
- Динамический анализ
  - Запуск контракта и проведения разного рода атак с целью выявление уязвимостей
- Code Review

Полученные данные

Рекомендация	**Тип**	**Приоритет**	**Вероятность возникновения**
Не найдено.			

A. Ошибки

Ошибок в данной редакции не найдено.

B. Замечания

Улучшения кода, рекомендованные в предыдущей редакции, были применены разработчиками в данной редакции.

C. Улучшения

Улучшения кода, рекомендованные в предыдущей редакции, были применены разработчиками в данной редакции.

Приложение. Классификация ошибок

Приоритет	
информационный	Этот вопрос не имеет прямого отношения к функциональности, но может иметь значение для понимания.
низкий	Этот вопрос не имеет никакого отношения к безопасности, но может повлиять на некоторое поведение неожиданным образом.
Средний	Проблема затрагивает некоторые функциональные возможности, но не приводит к экономически значимым потерям средств пользователей.
высокий	Эта проблема может привести к потере средств пользователя.
Вероятность	
низкий	Маловероятно, что система находится в состоянии, в котором ошибка могла бы произойти или могла бы быть вызвана какой-либо стороной.
Средний	Вполне вероятно, что эта проблема может возникнуть или быть вызвана какой-либо стороной.
высокий	Весьма вероятно, что эта проблема может возникнуть или может быть использована некоторыми сторонами.

Приложение. Цифровой отпечаток байткода

Аудит проведен для определенной версии кода на версии компилятора 0.5.10+commit.a1d534e с включённой оптимизацией.

Для того, чтобы проверить байт-код контракта на идентичность тому, который был проанализирован в процессе аудита необходимо:

1. Получить байт-код контракта (в любом обозревателе блоков)
2. Получить SHA1 от строки байткода
3. Сравнить с эталонной, в этом отчете

Sha1 от байткода: ab8c50bd67eb74fd685b1db03e53ed927cb19013

Проверить цифровой отпечаток

Приложение. Подпись заключения аудита


```
{
        "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",
        "msg": "В результате проведенного аудита не было выявлено
      замечаний, влияющих на безопасность средств пользователей,
      находящихся на контракте. Явные признаки экзит-скама – не
      обнаружены. (экзит скам - ситуация, при которой разработчики
      контракта имеют контролируемый доступ к средствам участников и могут
      без их ведома совершать операции вывода). Ошибок, брешей в
      безопасности так же не обнаружено. Telescr.in гарантирует
      безопасность и работоспособность контракта TRONexWorld. Актуально
      для байткода с sha1: ab8c50bd67eb74fd685b1db03e53ed927cb19013",
        "sig":
      "0x01f83c9d2c1432165fe95daee2a5da8eecb91e771af616c52d7d0a71db97b36a6
      e094928fd27762b5cc3c8e2b3a906cd14a26f31bb2ecae7b619bfdcb4597aa11c",
        "version": "3"
}
```


Проверить подпись