Аудит смарт-контракта TronApex

Редакция 2 от 03.12.2020

Telescr.in

Содержание

Краткая информация

Проект: tronapex.com
Сеть: TRON
Версия компилятора: 0.5.9
Оптимизация: включена
Дата аудита: 03.12.2020

Сведения

Проведён 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 были обнаружены ошибки, не влияющие напрямую на безопасность средств, но которые инвестору следует иметь в виду.

С полным списком обнаруженных проблем можно ознакомиться ниже.

Общее заключение

В результате проведенного аудита была выявлена 1 ошибка, не влияющая на безопасность средств пользователей, находящихся на контракте. Явные признаки экзит-скама – не обнаружены. Найденная ошибка связана с обработкой ограничений при выводе средств.

Telescr.in гарантирует безопасность и работоспособность контракта TronApex

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**
Неправильная обработка краевых значений	Ошибка	средний	низкий

A. Ошибки

1. Неправильная обработка краевых значений

В функции WithdrawDividends при проверке в каком диапазоне находится значение user.totalinvested, не учитывается его возможное равенство значениям WithdrawalDividendsRuleOneMax и WithdrawalDividendsRuleTwoMax.

B. Замечания

Не обнаружены.

C. Предупреждения

Не обнаружены.

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 0.5.9 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:
026187d694da024ba2fe4ab80e3303420162c5cb
Sha1 от байткода (без метаданных):
59b28a964383abbb66af09e2912535701f1c6dc6
Адрес контракта: TWehXUMJfpLduYrsqdhhvnMQwBzHKPrmSv

Проверить цифровой отпечаток

Приложение. Подпись заключения аудита


```
{
          "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",
          "msg": "В результате проведенного аудита была выявлена 1 ошибка, не влияющая на безопасность средств пользователей, находящихся на контракте. Явные
        признаки экзит-скама – не обнаружены. Найденная ошибка связана с обработкой ограничений при выводе средств. Telescr.in гарантирует безопасность и
        работоспособность контракта TronApex. Sha1 from bytecode: 026187d694da024ba2fe4ab80e3303420162c5cb Sha1 from bytecode (non-metadata):
        59b28a964383abbb66af09e2912535701f1c6dc6 Contract address: TWehXUMJfpLduYrsqdhhvnMQwBzHKPrmSv",
          "sig": "0x78cf0fde66566e71436fddb0e313d9f5c1ed21f9cd0c32d65277c80b14eeedb31fe6470f87ac1828b7b2603f126773fa43c9baf313b7d5353562b1ac0f4f23251b",
          "version": "3"
}
```


Проверить подпись