Аудит контрактов dANT

Редакция 1 от 20.12.2020

Telescr.in

Содержание

Краткая информация

Проект: dant.finance
Сеть: ETHEREUM
Версия компилятора: 0.6.2
Оптимизация: включена
Дата аудита: 20.12.2020

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 не было обнаружено ошибок, влияющих на безопасность средств.

Общее заключение

В результате проведенного аудита не было выявлено ошибок, влияющих на безопасность средств пользователей, находящихся на контракте. Явные признаки экзит-скама – не обнаружены.

Telescr.in гарантирует безопасность и работоспособность контрактов dANT.

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

Не обнаружены.

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:

7eeca3b6fcfea7d31d2436f91c863564e6c2099b – Token
5bca3bf4b747385b39f130253c8208403e95a371 - ReferralTree
a60eb902f776d547027de82b1f2709ec38204f42 - RewardsType0
7851090c149cbe94c3012fa554569312042e3893 – RewardsType1
8152b1c0ba1e86ac5dc08a7d92c73b89e82c37ae – RewardsType2
426276a57342380874dc5f3a22cee76e4d7c4f6d – MultisigWithTimelock

Sha1 от байткода (без метаданных):

811a0e7e55181375f808689079e243ce06dfac54 – Token
1f66bc317ec5321cf94b427594356b511b85c4a1 - ReferralTree
a21fd891c3f1f5c3d26316dfaccd29c82f2c4627 - RewardsType0
a99947de36a337a4cbd4fa5f6d66964aa32100c0 – RewardsType1
997f10a8c83053b2096c16b0f6be02d5e687adab – RewardsType2
ddf7ceecd33ba53b6f4aa8123a5560071e67db48 – MultisigWithTimelock

Адрес контракта:

0xbE3c393Fb670f0A29C3F3E660FFB113200e36676 – Token
0xe5C23851Bbde700414BeB3Ab2D2aE7063c8D9C72- ReferralTree
0x23D5caf6c288ab71B6061d97c9D8bEDa6f2Ef3ae - RewardsType0
0xBF8c3803A22C8Cf83005F73AF6FbD813a229251f – RewardsType1
0x3C58B7E291454e749B242F23A7A6a8A9f4dddDe9 – RewardsType2
0xE457D38074b5B8656707834C3Ae62D3158bdD847 - MultisigWithTimelock

Проверить цифровой отпечаток

Приложение. Подпись заключения аудита


```
{
          "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",
          "msg": "В результате проведенного аудита не было выявлено ошибок, влияющих на безопасность средств пользователей, находящихся на контракте. Явные
        признаки экзит-скама – не обнаружены. Telescr.in гарантирует безопасность и работоспособность контрактов dANT.
        0xbE3c393Fb670f0A29C3F3E660FFB113200e36676 – Token 0xe5C23851Bbde700414BeB3Ab2D2aE7063c8D9C72- ReferralTree 0x23D5caf6c288ab71B6061d97c9D8bEDa6f2Ef3ae
        - RewardsType0 0xBF8c3803A22C8Cf83005F73AF6FbD813a229251f – RewardsType1 0x3C58B7E291454e749B242F23A7A6a8A9f4dddDe9 – RewardsType2
        0xE457D38074b5B8656707834C3Ae62D3158bdD847 - MultisigWithTimelock",
          "sig": "0xde7c332cdd754b0b6e6fb013e1356e3fc7f97f54379b8f5502e4ad146f393dad60949c044ba0238174779986371c1bce0c087e6d95e45a66b9e45c6bf7edd9581b",
          "version": "3"
}
```


Проверить подпись