Аудит смарт контракта EthFinance

Date: 13th Ноября 2018
Version: 1.0

http://smartcontract.life
contacts@smartcontract.life

Классификация выявленных проблем

КРИТИЧНЫЕ - возможность кражи эфира/токенов или их блокировки без возможности восстановления доступа или иной потери эфира/токенов, причитающихся какой-либо стороне, например дивидендов.
СЕРЬЕЗНЫЕ - возможность нарушений работы контракта, при которых для восстановления его корректной работы необходима модификация состояния контракта вручную или его полная замена.
ПРЕДУПРЕЖДЕНИЯ - возможность нарушения запланированной логики контракта или возможность организации DoS-атаки на контракт.
ЗАМЕЧАНИЯ - все остальные замечания. Т.к. частно носят субъективный характер, не всегда обязательны к исправлению.

Методика аудита

Код контракта просматривается вручную на наличие известных уязвимостей, ошибок в логике, соответствие документации. При необходимости на сомнительные моменты пишутся автоматически тесты с использованием фреймворка truffle.

Выявленные проблемы

Адреса администрации (0x627306090abaB3A6e1400e9345bC60c78a8BEf57, 0xf17f52151EbEF6C7334FAD080c5704D77216b732) не являются смарт-контрактами, следовательно, дополнительной возможности приостановить инвестирование средств в контракт у владельцев нет.

Серьезные проблемы:

1. По условиям, описанным в тз, контракт работает до 150%, но проверка на достижение 150% реализована только в строках 118-123, которые сработают только если сумма выведенных дивидендов больше депозита. Следовательно, человек может получить сколько угодно выше % если не будет выводить дивиденды после преодоления 100% возврата депозита.
   При этом после вывода более 150% в строке 121 произойдет ошибка: из большей суммы будет вычтена меньшая, в результате чего случится переливание. И некорректная сумма будет записана в переменную amount, которая предназначена для совершения выплаты. Данная ошибка всегда будет останавливаться в строке 140, где safemath не позволит переливанию произойти еще раз. Следовательно, пользователь больше не сможет как выводить % так и переинвестировать средства.

2. По условиям, описанным в тз с одного кошелька можно вложить только 5 депозитов, но код контракта позволяет вложить 6 раз. Для исправления в строке 178 необходимо изменить <= на <.

Предупреждения:

1. В коде предусмотрена ситуация если инвестор укажет собственный адрес как реферера, но нет ограничения на указание рефererом адрес не являющийся инвестором, пользователь может указать свой любой другой адрес и получить 2% бонусов. Убрать данную лазейку можно добавив еще одно условие в строке 83: investor[referrer].deposit != 0

2. В языке написания смарт контрактов (солидити) не предусмотрены дробные числа, ввиду чего для избежания округления чисел выполняется сначала умножение, а после деление. (строки 84, 85, 91, 92, 97, 98, 118)

3. Библиотека SafeMath используется только в 8 строках смарт контракта, во всех данных случаях в контексте расчетов переливания быть не может. В целом, если все расчеты сделать правильными, то переливаний в контракте не будет, так как все входные данные – timestamp и суммы wei. Но тем не менее факт переливания в контракте найдет, поэтому рекомендуем переписать все вычисления на SafeMath.

Замечания:

1. Переменная owner не используется в коде и создана, по всей видимости, с единственной целью публичного отказа от владения смарт контракта. Строки 46, 66, 69-72 можно убрать.

2. Две переменные addresses и countsInvestors делают в коде одну и ту же функцию: подсчет инвесторов. Для записи в обе переменные расходуется газ. Подсчет количества инвесторов можно заменить логгированием нового инвестора, далее логи можно собирать с езерскана и получать необходимое значение.
+ в случае полной выплаты происходит полное удаление записи об инвесторе, следовательно, если он второй раз инвестирует в проект, в обеих переменных он будет прибавлен как новый инвестор.

3. В 96 и 98 строках происходит умножение на 100, а затем деление на 100.

4. В переменную fee сохраняется совокупная сумма вложенных средств в контракт, но слово fee с английского переводится как комиссия, следовательно, название не отражает сути переменной.