Аудит смарт контракта EthereumHyipBlitz

Date: 27th Октября 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

КРИТИЧНЫЕ

Бэкдоров, уязвимостей и критических ошибок в контракте **не обнаружено**.

Адрес админа (0x6c7abcac75508430bd9d2a558c5733945b528f56) не является смарт-контрактом, следовательно, дополнительной возможности приостановить инвестирование средств в контракт у владельцев нет.

СЕРЬЕЗНЫЕ

Не выявлены

ПРЕДУПРЕЖДЕНИЯ:

1. При реинвесте пользователь теряет все свои невыведенные дивиденды.

2. Установленный минимум на вывод средств, затрудняет пользователям лично убедиться в работоспособности контракта с помощью инвеста небольшой суммы. Те, кто проинвестируют 0.01 эфира будут вынуждены ждать 25 дней до первой возможности вывести дивиденды.
3. Адресом реферера можно указать самого себя, получив при этом бонус 3%. Также несмотря на предусмотренное закрепление реферера за инвестором, пользователь в любой момент может сменить его, в том числе на себя.

ЗАМЕЧАНИЯ:

1. Переменная adminAddress (строка 47) не используется в контракте.
2. Функция getRefer (строки 96-100) является публичной и доступна в интерфейсе контракта. Ее название вводит в заблуждение, так как по смыслу названия можно подумать, что для введенного адреса инвестора она вернет адрес его реферера. Рекомендуем сменить видимость функции на private или internal.
3. Функцию getPercent (строка 66-69) можно было заменить обычной переменной. Также в этой функции возвращается значение умноженное на 100, чего можно было избежать, поделив множитель 10000 на 100 в формуле вычисления дивидендов (строка 98).
4. Переменная active (строка 37) необязательна, ее запись (строка 127) только увеличивает стоимость транзакций. Все строки ее использования (115 и 132) можно было заменить проверками на наличие amount или atBlock пользователя.

Описание функционала:

Контракт предоставляет возможность любому пользователю инвестировать ETH (от 0.01) в проект (отправить эфир на адрес контракта) и получить возможность выводить 4% от своей суммы каждые 5900 блоков (~ 1 день). Вывод дивидендов осуществляется отправкой 0 эфиров на контракт и возможен только после накопления 0.01 ETH к выводу, и далее в любой момент времени.

Реинвест в проект осуществляется отправкой эфира на адрес контракт. При реинвесте все невыведенные дивиденды теряются.

Также в проекте присутствует реферальная программа. Указывать реферера нужно в поле data при инвестировании средств. При условии, если реферер является участником проекта, он автоматически получит 3% от внесенной рефералом суммы. При дальнейших реинвестах

пользователя реферер будет получать по 3%. Пользователь может изменить реферера при любом реинвесте. Также пользователь может указать самого себя в качестве реферера.

В контракте есть 4 инфофункции:
ShowDeposit – возвращает сумму инвестиции в проект по конкретному кошельку.
ShowLastChange – возвращает время последнего инвеста, реинвеста или вывода дивидендов в UNIX Time.
ShowUnpayedPercent – возвращает начисленные к выводу дивиденды.
GetRefer – внутренняя функция контракта не имеющая ценности для пользователей.