Владимир Сергеевич @ProRunner
Пользователь

сегодня в 00:16

Критическая уязвимость в multisig кошельке Parity, хакерами выведен $31 миллион в ethereum

Криптография*, Информационная безопасность*

Из-за уязвимости в коде смарт-контракта multisig кошелька Parity (1.5 и более поздний) хакер смог вывести монет ethereum в эквиваленте 31 миллиона долларов.

Объяснение механизма атаки вкратце: функция initWallet() в коде, позволяющая определить владельца кошелька, оказалась публичной, и её мог вызвать любой человек. После переопределения владельца оставалось только перевести деньги. Более полное объяснение (на англ.)

Кошелёк хакера: etherscan.io/address/0xb3764761e297d6f121e79c32a65829cd1ddb4d32
(уже начался перевод средств на другие адреса)

White-hat группа смогла вывести эфира в 76 миллионов долларов (и ещё 80 миллионов в различных токенах) с уязвимых кошельков для защиты средств
etherscan.io/address/0x1dba1131000664b884a1ba238464159892252d3a

Были украдены деньги с кошельков следующих ICO:

- Edgeless Casino
- Swarm City
- aeternity blockchain

> "Edgeless casino, swarm city, and aeternity have all been drained" --CF Slack #parityhack
> — CoinFund (@coinfund_io) July 19, 2017

В white-hat кошельке на данный момент, например, находятся токены eos криптовалютного инвестиционного фонда satoshi.fund в размере $1,5 млн.

Multisig (мульти-подпись) кошелек в теории должен был предоставить дополнительную защиту из-за требования подписи нескольких человек для операции со средствами.

Оповещение об уязвимости в блоге Parity
Официальное заявление Swarm City, подтверждающее потерю 44,055 ETH.

> invested in Aeternity
> lol
> and they lost like 18million
> f#$@ morons…
>
> It looks like it will be a eternity until you get your money back ;)

The DAO 2.0. Только хард-форка эфира для спасения средств в этот раз не ожидается. Твит Виталика Бутерина в ответ на вопрос, почему был произведен хард-форк цепи ethereum в случае с The DAO, а здесь его не будет:

> 1. Ecosystem less mature then
> 2. More at stake then as % of all ETH
> 3 [most impt]. Today's attacker can just move funds, so HF is impossible
> — Vitalik Buterin (@VitalikButerin) July 19, 2017

1. Менее зрелая экосистема в то время
2. Тогда на кону был больший % от всего ETH
3. (самое важное) Хакер может просто перевести средства, поэтому хард-форк невозможен

ethereum, parity, aeternity, swarm city, это вам не баян, надо срочно придумать своё ICO

ПОХОЖИЕ ПУБЛИКАЦИИ

20 сентября 2016 в 12:37
Вам не хватает скорости R? Ищем скрытые резервы
+6 3,6k 38 11

10 июня 2016 в 14:03
Расследование: куда ваш сайт редиректит пользователей, а вы об этом даже не подозреваете
+17 36,6k 67 42

9 февраля 2016 в 10:32
Как быть, если вы не знаете, что делать со своей жизнью
+2 8,1k 38 3

САМОЕ ЧИТАЕМОЕ Разработка

Сутки Неделя Месяц

Как ЕА усложнили нам жизнь, или как мы чинили баг 12-летней давности
+48 98k 52 29

Критическая уязвимость в multisig кошельке Parity, хакерами выведен $31 миллион в ethereum
+22 8,9k 19 12

Книга «Python. Уроки»
+25 9,8k 129 19

K-sort: новый алгоритм, превосходящий пирамидальную при n <= 7 000 000
+18 6,5k 66 3

Яндекс открывает технологию машинного обучения CatBoost
+207 27,9k 295 98

Комментарии (13)

Shador 20 июля 2017 в 02:57 +1

Не "Больше на кону, чем просто % от всего ETH", а "Тогда на кону был больший % от всего ETH".

iNickname 20 июля 2017 в 06:50 0

Не согласен.
Скорее всего имеется ввиду репутация и т.п. сейчас.

ЧТО ОБСУЖДАЮТ

Сейчас Вчера Неделя

Критическая уязвимость в multisig кошельке Parity, хакерами выведен $31 миллион в ethereum

ProRunner 20 июля 2017 в 07:29 +1

Да нет, думаю @shador прав. Я then с than перепутал при переводе. Виталик говорил про «больше на кону в то время»

FenixFly 20 июля 2017 в 07:15 0

А можно запретить всей системе проводить операции с этим кошельком? Пусть хоть миллиард украдут, воспользоваться все равно не смогут.

ProRunner 20 июля 2017 в 07:40 +1

То, о чем вы говорите, и есть хард-форк сети. Он и был произведен в случае со взломом The DAO, из-за чего произошёл раскол сети эфира на ETH и ETC.

Но в случае с The DAO у сообщества было значительное время до того, как хакер смог бы воспользоваться деньгами. Здесь, как Виталик и говорил, хакер может просто перевести деньги (например, через какой-нибудь eth-миксер), так что отследить их дальнейшую судьбу будет невозможно.

zagayevskiy 20 июля 2017 в 12:15 0

долбодятлы сами виноваты, имхо

ProRunner 20 июля 2017 в 14:19 0

Кто? Разработчики кошелька или пользователи? Разработчики несомненно, но пострадали-то не они.

Если пользователи, то извините, давайте хакер найдет уязвимость в какой-нибудь программе, которой вы пользуетесь, и уведет с вашего банковского счета все ваши накопления. Тоже долбодятлом будете себя считать?

kisskin 20 июля 2017 в 07:15 +12

ага, давайте каждый раз, как какой-то банк ограбят, будем новые деньги вводить.

Enam 20 июля 2017 в 14:36 0

Потребительские вклады в банках обычно застрахованы, как и личные средства банков.

potan 20 июля 2017 в 07:47 0

Ошибка была в коде конкретного контракта, или в коде кошелька?

ProRunner 20 июля 2017 в 08:18 +1

Насколько я понимаю, хранилище кошелька представляет собой адрес смарт-контракта в сети эфира, поэтому можно сказать в коде всех смарт-контрактов, созданных с помощью Parity.

yurisv3 20 июля 2017 в 08:16 +9

шо? никогда ж такого не было, и вот опять?!

404 amarao 20 июля 2017 в 11:58 +1

Супер умные но не супер надёжные контракты.

Только полноправные пользователи могут оставлять комментарии. Войдите, пожалуйста.

ИНТЕРЕСНЫЕ ПУБЛИКАЦИИ

Особенности национальной SMS-авторизации
+10 1,1k 5 4

Google планирует представить облачный сервис для квантовых вычислений
+5 954 7 1

Ядро автоматизации тестирования в микросервисной архитектуре
+10 1,4k 14 0

Когда деревья были большими: как маленький дата-центр ураган пережил
+20 2,7k 12 4

Deep Learning, теперь и в OpenCV
+19 2,6k 48 5

Дели — сокращай, или как мы делали мобильный 2ГИС Онлайн
2,6k 10

Синхронизация Vivaldi: ответы на вопросы
6,3k 16

Вы ни черта не понимаете в цветах
24,4k 181

Выбранный UI-фреймворк – вред. Архитектурные требования – профит
1,7k 4