протокола Ordinals в 2022 г. Добавление в список NVD означает, что уязвимость признана важной для информирования общественности.

В декабре 2023 г. новая функция в блокчейне Ethereum Create2 стала причиной кражи $60 млн. Злоумышленники нашли способ обойти системы безопасности криптовалютных кошельков, используя функцию, которая позволяет создавать смарт-контракты в блокчейне, причем с возможностью предварительного расчета их адресов до развертывания. Функция является легитимной, но она создала уязвимости в системе безопасности Ethereum. Основной способ эксплуатации заключается в создании новых адресов контрактов без истории подозрительных транзакций. Злоумышленники заставляют жертвы подписывать вредоносные транзакции, после чего переводят активы на предварительно рассчитанные адреса.

В декабре 2023 г. многие криптосервисы оказались под угрозой из-за взлома кода кошелька Ledger. Уязвимость была исправлена, но успела затронуть несколько популярных децентрализованных сервисов, администраторы которых вынужденно отключили пользовательский интерфейс. Оказался скомпрометированным широко используемый код сервиса авторизации через криптокошелек Ledger. Компания сообщила, что им удалось удалить вредоносный код, но уязвимость эксплуатировалась в течение двух часов и распространялась на большинство популярных децентрализованных криптосервисов.

Как видно из этого выборочного списка, эксплуатация практически любой уязвимости в криптокошельках или криптопротоколах немедленно ведет к эксплуатации финансовых рисков.

Управление уязвимостями

Когда речь идет о контроле уязвимостей при эксплуатации криптовалютных кошельков, рекомендации всегда тривиальны, но от этого они не становятся менее важными.

1. Использование надежных кошельков. Выбор надежного и проверенного криптовалютного кошелька с хорошей репутацией снижает риск возникновения уязвимостей и кибератак.

2. Обновление системы и программного обеспечения. Регулярные обновления кошельков и всех связанных с ними программных компонентов помогают устранять известные уязвимости и обеспечивают безопасность системы.

3. Многофакторная аутентификация. Включение функции многофакторной аутентификации обеспечивает дополнительный уровень защиты от несанкционированного доступа к кошельку.

4. Резервное копирование и безопасное хранение ключей. Регулярное создание резервных копий ключей доступа к кошельку и их безопасное хранение в надежном месте поможет избежать потери средств в случае утери или повреждения исходного кошелька.


Изображение: playground.com

5. Обучение. Проведение обучающих мероприятий по безопасности криптовалютных кошельков поможет пользователям понять основные угрозы и принять меры по их минимизации.

Другими словами, чтобы минимизировать угрозы, рекомендуется использовать надежные и проверенные криптовалютные кошельки, следовать правилам кибергигиены и передовому опыту в сфере безопасности, таким как использование сложных паролей, установка двухфакторной аутентификации, резервное копирование закрытого ключа и резервной фразы, их хранение в надежном месте. Необходимо также проявлять бдительность и повышенное внимание при работе с криптовалютными операциями и подозрительными запросами.

Есть улучшения и в сфере стандартизации: в качестве примера можно привести механизм BIP (Bitcoin Improvement Proposal), используемый для предложения изменений в протокол биткоина. Предложения в рамках BIP разрабатываются членами сообщества, включая разработчиков, исследователей и пользователей, и предназначены для обсуждения и координации изменений в сети.

Обратим внимание на предложение BIP-0039 (обычно называемое просто BIP39) – это стандарт, определяющий метод генерации мнемонических фраз для создания и восстановления кошельков биткоин и других криптовалют.

Мнемоническая фраза (Seed Phrase) представляет собой набор слов, который можно легко запомнить и использовать для восстановления частного ключа кошелька. Этот стандарт был предложен для упрощения процесса резервного копирования и восстановления кошельков, а также для повышения безопасности, предоставляя пользователю удобный способ резервного копирования и хранения секретной информации.

Мнемонические фразы по BIP39 особенно полезны для создания и использования кошельков с использованием множества криптовалют, так как они обычно поддерживаются большинством кошельков и платформ.

Замечания в заключение

Необходимо развивать взаимодействие и взаимную поддержку внутри сообщества по вопросам безопасности и устранения уязвимостей для повышения уровня безопасности криптоплатформ и криптосервисов.

Важным аспектом применения блокчейн-технологий стал запущенный в России цифровой рубль. К счастью, для него практически все, что было известно к моменту запуска, было учтено. Но остается важным вопрос операционной безопасности и повышения осведомленности граждан. Об этом требуется особая забота.

Все чаще злоумышленники используют фишинговые транзакции, фишинговые аирдропы (NFT), вредоносные смарт-контракты на сайтах для последующего опустошения криптовалютных кошельков. Это стало возможным ввиду доступности инструментов широкому кругу злоумышленников.

И конечно же, уже сегодня необходимо готовиться к грядущей квантовой угрозе, путем разработки квантовоустойчивых протоколов и технологий. В перспективе года-двух злоумышленникам могут стать доступны квантовые алгоритмы перебора ключей. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru