Google, Microsoft, AWS и другие крупнейшие игроки подвержены масштабной утечке кода.

Palo Alto Networks обнаружила уязвимости в процессах CI/CD ряда известных открытых проектов, включая разработки Google – одна из крупнейших технологических компаний в мире, основанная в 1998 году в США. Основной продукт компании – поисковая система Google, которая позволяет находить информацию в интернете. Компания также разрабатывает множество других продуктов, таких как электронная почта Gmail, видеохостинг YouTube, карты Google Maps и операционную систему Android для мобильных устройств. Google является одним из лидеров в области искусственного интеллекта и облачных вычислений. Компания занимает высокие позиции в рейтингах лучших работодателей в мире.
" data-html="true" data-original-title="Google" >Google, Microsoft, AWS и Red Hat. Проблема связана с утечкой GitHub — это платформа для хостинга и совместной разработки программного обеспечения.

 Одним из ключевых аспектов GitHub является его социальная составляющая. Разработчики могут подписываться на интересующие их проекты, следить за обновлениями, вносить свои предложения и комментарии, а также взаимодействовать с другими разработчиками, делая процесс разработки быстрее и эффективнее.

 GitHub является популярным инструментом в сообществе разработчиков и служит платформой для сотен тысяч открытых и закрытых проектов в различных областях программного обеспечения." data-html="true" data-original-title="GitHub" >GitHub-токенов, которые могут быть использованы для несанкционированного доступа к приватным репозиториям, кражи исходного кода или внедрения вредоносного ПО.

Токены попадают в артефакты по причине сочетания нескольких факторов: небезопасные настройки по умолчанию, ошибки в конфигурации со стороны пользователей и недостаточная проверка безопасности на этапе настройки рабочих процессов в GitHub. Одним из ключевых элементов проблемы стала широко используемая в рабочих процессах GitHub функция «actions/checkout», которая клонирует код репозитория, делая его доступным для выполнения рабочих процессов.

Артефакт, созданный GitHub Actions

По умолчанию функция сохраняет Токен — это специальная метка или код, который используется в системах авторизации для подтверждения легитимности пользователя и предоставления доступа к определенным ресурсам. Токены могут быть физическими (например, смарт-карты или ключи безопасности) или виртуальными (например,

одноразовые пароли), и они усиливают безопасность системы, так как предоставляют дополнительный уровень аутентификации и контроля доступа." data-html="true" data-original-title="Токен" >токен в локальной директории .git. Если директория случайно загружается в виде артефакта, токен становится доступным для посторонних. Кроме того, в каталоге могут храниться другие чувствительные данные, такие как API-ключи и токены доступа к облачным сервисам.

Публично представленный токен GitHub

Проблема усугубляется тем, что артефакты, сгенерированные в процессе CI/CD, такие как результаты сборок и тестов, могут храниться и быть доступными в течение 3 месяцев. Ещё одним риском являются переменные окружения, используемые в конвейерах CI/CD для хранения токенов GitHub. Такие переменные могут случайно записываться в логи, становясь доступными через артефакты.

В результате атаки на утекшие токены злоумышленник может эксплуатировать различные сценарии состояния гонки (Race Condition — это так называемое состояние гонки между несколькими процессами за доступ к какому-либо ресурсу или за право изменить определенное значение.

 Если две программы одновременно пытаются изменить одно и то же значение в памяти компьютера или получить доступ к одному и тому же файлу, это может привести к непредсказуемым ошибкам в системе.

 Разработчики стараются избегать этого состояния при написании программ, используя различные механизмы синхронизации или блокировки, которые, например, допускают к ресурсам только один процесс, блокируя все остальные." data-html="true" data-original-title="Race Condition" >race condition), пытаясь извлечь и использовать токены до истечения их срока действия. Токены GitHub действительны на протяжении выполнения рабочего процесса, и возможность их использования зависит от конкретного случая. Например, токен «Actions_Runtime_Token», используемый GitHub для управления кэшированием и артефактами, обычно активен в течение 6 часов, что ограничивает время для атаки.

Цепочка атаки

Palo Alto Networks выявила 14 крупных open-source проектов, в которых произошла утечка токенов, и сообщила разработчикам. Среди проектов — Firebase (Google), OpenSearch Security (AWS), Clair (Red Hat), JSON Schemas (Microsoft) и другие.

Пользователям GitHub рекомендуется пересмотреть настройки своих CI/CD-процессов, избегать загрузки целых директорий в артефакты, очищать логи и регулярно проверять конфигурации. Также важно установить минимально необходимые права доступа для токенов, чтобы снизить риски в случае их утечки.

Несмотря на то, что Palo Alto Networks выявила оишбки, основные проблемы остаются нерешенными, поскольку GitHub решил не устранять риск, возложив ответственность за защиту артефактов на пользователей. Учитывая сложившуюся ситуацию, пользователям GitHub необходимо осознать риски, оценить свою уязвимость и принять меры для предотвращения утечек в будущем.

Пользователям настоятельно рекомендуется пересмотреть настройки своих конвейеров CI/CD, избегать включения целых директорий в артефакты, очищать логи и регулярно проводить ревизию конфигураций рабочих процессов. Также следует изменить настройки по умолчанию для действий, подобных «actions/checkout», чтобы предотвратить сохранение токенов и других чувствительных данных. Установка минимально необходимых прав доступа для токенов, используемых в рабочих процессах, также поможет снизить возможный ущерб в случае утечки.