Почему владельцы уязвимой платформы упорно не хотят исправлять найденную ошибку?

Исследовательская группа Cybernews — это информационное издание, которое занимается освещением проблем информационной безопасности. Они публикуют новости, статьи, аналитику и исследования, касающиеся различных аспектов кибербезопасности, включая уязвимости в ПО, кибератаки и защиту данных. Cybernews также предоставляют информацию о технологиях защиты и направлениях развития индустрии кибербезопасности." data-html="true" data-original-title="Cybernews" >Cybernews обнаружила утечку данных клиентов, использующих популярные турецкие сервисы доставки еды. Инцидент связан с компанией Paketle Lojistik Hizmetleri, которая занимается маршрутизацией заказов через платформу на базе Apache Kafka — это распределенная платформа потоковой передачи данных, разработанная для построения высокопроизводительных и отказоустойчивых систем обработки данных в реальном времени.

 Kafka позволяет публиковать, подписываться на потоки данных, хранить их и обрабатывать, предоставляя при этом возможности масштабирования и отказоустойчивости.

 В основе Kafka лежит модель публикации/подписки, где данные организованы в топики. Производители (publishers) отправляют сообщения в топики, а потребители (consumers) подписываются на топики и читают сообщения. Благодаря этому Kafka широко используется для интеграции различных приложений и микросервисов, а также для построения систем обработки потоков данных и логов." data-html="true" data-original-title="Kafka" >Kafka, не обеспечивая должный уровень безопасности.

На вышеупомянутой платформе доступен обширный перечень личных данных клиентов, такие как имена, домашние адреса, номера телефонов, электронная почта, детали заказов, IP-адреса и токены аутентификации. Эта информация доступна всем, кто подключается к системе, без какой-либо аутентификации.

«Каждый раз при поступлении нового заказа любой посторонний может узнать чувствительную информацию о любом клиенте», — заявили исследователи Cybernews. «В настоящий момент система представляет из себя фонтан, разбрызгивающий персональные данные».

Исследователям удалось найти заказы, размещённые через следующие турецкие приложения для доставки еды:

Специалисты Cybernews сообщили о своей находке представителям Paketle Лojistik Hizmetleri, а также турецким властям, включая местную команду реагирования на

компьютерные инциденты. Несмотря на восемь писем, отправленных между 25 января и 4 марта 2024 года, компания не приняла мер для устранения уязвимости. На момент публикации материала доступ к уязвимым Kafka-инстансам оставался открытым.

Платформа хранит данные о заказах за последние десять дней, а новые добавляются буквально каждую минуту. В течение года злоумышленники могли получить доступ к более чем 3 миллионам уникальных заказов.

Эта утечка создаёт серьёзную угрозу для безопасности турецких клиентов. Злоумышленники могут использовать эти данные для раскрытия местоположения, кражи заказов, подделки курьеров, фишинговых атак и других киберпреступлений. Также пострадать могут и рестораны, интегрированные в систему Paketle, которые могут подвергнуться фальсификации заказов и хаосу в работе.

Исследователи Cybernews подчёркивают необходимость срочного устранения уязвимости. Платформодержателям рекомендуется внедрить систему аутентификации, настроить белые списки IP-адресов, применить шифрование SSL/TLS, а также механизмы мониторинга для обнаружения и реагирования на подозрительную активность.