Простой баг стал отправной точкой для масштабной кибератаки.

В популярной системе GPS (Global Positioning System) – это глобальная система спутниковой навигации, предоставляющая информацию о местоположении и времени в любой точке Земли или над её поверхностью. Она состоит из сети спутников, которые постоянно передают сигналы, и приемника, который используется для определения точного местоположения на основе этих сигналов. GPS применяется в навигационных системах, автомобильных навигаторах, мобильных устройствах и во многих других областях, где требуется точное определение координат.
" data-html="true" data-original-title="GPS" >GPS-трекинга Traccar – это система отслеживания GPS-устройств с открытым исходным кодом, которая позволяет в реальном времени контролировать местоположение различных объектов. Программное обеспечение Traccar поддерживает широкий спектр GPS-трекеров и протоколов, обеспечивая удобное отображение данных на карте. Благодаря веб-интерфейсу и мобильным приложениям, пользователи могут легко мониторить объекты с любого устройства. Traccar идеально подходит как для личного использования, так и для коммерческих задач, таких как управление автопарком и контроль за перемещением транспортных средств." data-html="true" data-original-title="Traccar" >Traccar, используемой как для личного, так и корпоративного применения, обнаружены две критические уязвимости, которые могут привести к удалённому выполнению кода. Уязвимости, обозначенные как CVE-2024-31214 и CVE-2024-24809, позволяют неавторизованным злоумышленникам выполнять атаки, если включена функция регистрации гостей, которая по умолчанию активирована в версии Traccar 5.

Traccar, приложение на основе Java – язык программирования, который был разработан компанией Sun Microsystems. Приложения Java, как правило, компилируются в специальный байт-код, что позволяет им работать на любой виртуальной Java-машине в независимости от компьютерной архитектуры. Байт-код не зависит от операционной системы и оборудования и позволяет выполнять Java-приложения на любом устройстве, для которого существует соответствующая виртуальная машина." data-html="true" data-original-title="Java" >Java, использует сервер Jetty для обработки запросов. В версии Traccar 5.1 была добавлена функция загрузки изображений для устройств, которая и стала причиной уязвимости. Обе проблемы связаны с обработкой загрузки изображений устройств, где злоумышленники могут манипулировать именем файла и расширением, используя технику обхода каталогов (Path Traversal (Directory Traversal) представляет собой уязвимость, которая позволяет злоумышленнику получить доступ к файлам и директориям, находящимся за пределами предполагаемой корневой директории веб-

сервера.

 Эксплуатация достигается путем манипулирования переменными, которые ссылаются на файлы (например, через URL-запросы), используя специальные последовательности символов, такие как "../" (возвращающиеся на уровень выше в структуре каталогов).

 Таким образом, хакер может обойти ограничения доступа и читать, а иногда и изменять файлы, к которым обычно доступ ограничен. Недостаток позволяет получить несанкционированный доступ к конфиденциальным данным." data-html="true" data-original-title="Path Traversal" >Path Traversal). Это позволяет размещать файлы в произвольных местах на файловой системе, что в конечном итоге может привести к выполнению вредоносного кода на сервере.

Одним из возможных сценариев атаки является загрузка crontab-файла на серверы, работающие на базе Linux, что позволит злоумышленнику получить обратную оболочку (Reverse Shell (обратная оболочка) — техника, при которой злоумышленник создаёт программу или скрипт на своей системе и размещает её на целевой системе. Затем, когда целевая система запускает эту программу, она пытается подключиться обратно к злоумышленнику. Если соединение установлено успешно, злоумышленник получает удалённый доступ и полный контроль над целевой системой." data-html="true" data-original-title="Reverse Shell" >Reverse Shell). Другие методы включают загрузку вредоносного модуля ядра или создание вредоносных правил udev, которые также приводят к удалённому выполнению кода при перезагрузке или входе пользователя в систему.

На Windows-системах уязвимость может быть использована для размещения вредоносного ярлыка в папке автозагрузки, что приводит к выполнению команды при каждом входе в систему.

Проблема была обнаружена исследователями из Horizon3 — это компания, которая занимается разработкой и производством программного обеспечения для систем кибербезопасности. Они создают продукты, которые помогают компаниям защищаться от киберугроз и обнаруживать их на ранней стадии. Их продукты включают в себя системы антивирусной защиты, детекторы вторжений, мониторинг сетей и другие решения, которые помогают защитить корпоративные сети и данные от киберпреступности. Они также предлагают консультационные услуги и обучение, чтобы помочь клиентам улучшить защиту информации." data-html="true" data-original-title="Horizon3" >Horizon3, которые сразу сообщили об уязвимостях разработчикам. В Traccar 6 эти уязвимости были исправлены, а функция регистрации гостей была отключена по умолчанию, что значительно улучшило безопасность системы.

Для защиты своих систем пользователям рекомендуется как можно скорее обновиться

до Traccar 6 или отключить функцию регистрации гостей. Кроме того, если сервер уже был скомпрометирован, необходимо быть осторожным при перезагрузке системы, так как это может активировать заложенные вредоносные программы.

На момент обнаружения уязвимостей около 1400 серверов Traccar версии 5 были открыты в сети с уязвимыми настройками по умолчанию. Пользователям рекомендуется проверить свои системы и принять необходимые меры для предотвращения возможных атак.