Исследователи обнаружили способ, как хакеры могут использовать устройства в качестве инструмента взлома.

Серия уязвимостей в модемах Cox Communications могла стать отправной точкой для злоумышленников, желающих получить несанкционированный доступ к устройствам и выполнять вредоносные команды. Исследователь безопасности из Yuga Labs Сэм Карри опубликовал новый доклад, в котором подробно описал потенциальные угрозы, связанные с уязвимостями в модемах Cox.

Уязвимости показали, как удаленный злоумышленник без каких-либо предварительных условий мог бы выполнять команды и изменять настройки миллионов модемов Cox, получать доступ к персональной информации бизнес-клиентов и, по сути, обладать теми же правами, что и служба поддержки интернет-провайдера, как говорится в отчете исследователя.

После ответственного раскрытия информации 4 марта уязвимости были оперативно устранены американским провайдером широкополосного интернета Cox в течение 24 часов. На данный момент нет данных о том, что эти уязвимости были использованы в реальных атаках.

Карри признался, что был сильно удивлен практически неограниченным доступом, который интернет-провайдеры, такие как Cox, имеют к устройствам своих клиентов. Агенты поддержки Cox имеют возможность удаленно управлять настройками устройств, такими как изменение пароля Wi-Fi и просмотр подключенных устройств, используя протокол TR-069.

Анализ Карри выявил около 700 открытых конечных точек API (Application Programming Interface) — это набор готовых функций и процедур, которые позволяют разработчикам создавать программное обеспечение, взаимодействующее с другими приложениями или сервисами. API определяет, как различные компоненты программного обеспечения должны взаимодействовать друг с другом, обеспечивая при этом безопасность и стабильность работы системы. API часто используется в веб-разработке для создания сайтов и приложений, которые используют данные и функциональность других сервисов." data-html="true" data-original-title="API" >API в модемах Cox, некоторые из которых могли быть использованы для получения административных прав и выполнения несанкционированных команд путем использования проблем с разрешениями и многократного воспроизведения HTTP-запросов.

Среди них была конечная точка «profilesearch», которую можно было эксплуатировать для поиска клиента и получения данных его бизнес-аккаунта, используя только имя, многократно воспроизводя запрос. Также можно было получить MAC-адреса подключенного оборудования на аккаунте и даже получить доступ к бизнес-аккаунтам и изменять их настройки.

Еще более тревожным оказался тот факт, что можно было перезаписать настройки устройства клиента, если злоумышленник обладал криптографическим секретом, необходимым для обработки запросов на модификацию оборудования. Таким образом хакер мог перезагрузить устройство, получить доступ к роутеру и выполнять команды на нём.

В гипотетическом сценарии атаки злоумышленник мог бы использовать эти API для поиска клиента Cox, получения полных данных его учетной записи, запроса MAC-адреса оборудования для извлечения паролей Wi-Fi и подключенных устройств, а также выполнения произвольных команд для захвата учетных записей.

Карри объясняет, что проблема, вероятно, возникла из-за сложностей управления клиентскими устройствами. Создание REST API, который может универсально общаться с сотнями различных моделей модемов и роутеров – действительно сложный процесс. Если бы в Cox изначально увидели в этом необходимость, могли бы встроить механизм авторизации, который не полагался бы на один внутренний протокол с доступом к стольким устройствам. Это достаточно сложная задача.

Ранее Карри совместно с несколькими другими исследователями ранее раскрыл несколько уязвимостей, затрагивающих миллионы автомобилей 16 различных производителей, которые можно использовать для разблокировки, запуска и отслеживания автомобилей.