В чьих руках CVE-2024-3661 представляет наибольший риск для общественности?

6 мая исследователь из Leviathan Security Group – американская компания, специализирующаяся на кибербезопасности. Она предоставляет услуги в областях оценки уязвимостей, пентестинга, консалтинга и исследования безопасности. Компания известна своими исследованиями в сфере безопасности информационных технологий и помогает организациям защищаться от кибератак. Leviathan Security акцентирует внимание на комплексном подходе к защите данных и инфраструктуры своих клиентов." data-html="true" data-original-title="Leviathan Security" >Leviathan Security обнаружил критическую уязвимость в системе Virtual Private Network (VPN (Virtual Private Network, виртуальная частная сеть) – это технология, которая создаёт защищенное и зашифрованное соединение между Интернетом и конечным устройством. Она используется для обеспечения конфиденциальности, безопасности и анонимности в сети." data-html="true" data-original-title="VPN" >VPN), названную TunnelVision (CVE-2024-3661). Эта уязвимость позволяет злоумышленникам обходить шифрование VPN и перенаправлять сетевой трафик за пределы VPN-туннеля, что приводит к его незащищённости.

TunnelVision работает за счёт использования протокола динамической конфигурации хоста (DHCP (Dynamic Host Configuration Protocol) — это сетевой протокол, позволяющий автоматически присваивать устройствам IP-адреса и другие сетевые параметры при подключении к сети. Протокол обеспечивает простое и автоматическое взаимодействие устройств с сетью без необходимости ручной настройки каждого устройства. В больших сетях, где устройства регулярно подключаются и отключаются, DHCP существенно упрощает процесс управления IP-адресацией." data-html="true" data-original-title="DHCP" >DHCP). Злоумышленники создают побочный канал, через который нешифрованный трафик направляется на их серверы, обходя VPN-туннель. VPN-клиент продолжает считать, что данные передаются через защищённый туннель, в то время как они уже находятся вне его.

Спустя время после выхода уязвимости многие эксперты высказались на тему того, что считают опасность TunnelVision преувеличенной. Так, доктор Питер Мэмбри, главный инженер ExpressVPN, отметил:

«Провести атаку не так просто, как описано. Она требует нескольких условий для успешного выполнения. Например, атака возможна только в общественных Wi-Fi сетях. В домашней или офисной сети вы не будете уязвимы. Также существуют защиты, которые могут быть установлены провайдерами общественных Wi-Fi».

Другие эксперты указывают, что для успешного проведения атаки необходимо, чтобы маршрутизатор пользователя был взломан. Таким образом, VPN-клиент остаётся защищённым, если сеть не была атакована на локальном уровне или если используется публичный Wi-Fi. Также безопасность обеспечивается использованием VPN killswitch и встроенных файрволов.

Уязвимость TunnelVision предоставляет новую возможность для атак на локальные сети с целью деанонимизации VPN-трафика. С активным распространением протокола HTTPS, хакерам стало сложнее перехватывать сетевой трафик. Однако, если злоумышленник получит доступ к локальной сети, это создаст оптимальные условия для эксплуатации уязвимости TunnelVision.

На данный момент эксперты считают, что опасность TunnelVision преувеличена, поскольку условия для её успешной реализации достаточно сложны. Однако, если такая уязвимость попадёт в руки западных спецслужб, это наверняка откроет для них новые пути для деанонимизации пользовательских данных.

История показывает, что государственные агентства ранее неоднократно использовали уязвимости для незаконного слежения за пользователями. Так, в декабре прошлого года сенатор США Рон Уайден раскрыл информацию о том, что правоохранительные органы США проводят слежку без ордера за пользователями Apple и Android через уязвимость в push-уведомлениях.

Из других подобных случаев, уязвимость EternalBlue, обнаруженная Агентством национальной безопасности США (АНБ), была использована для взлома Windows-систем без уведомления Microsoft. Это позволило АНБ проводить несанкционированные вторжения, пока группа хакеров Shadow Brokers не раскрыла эту информацию.

История Эдварда Сноудена также напоминает о масштабах незаконных программ слежения АНБ. Такие случаи показывают, что уязвимости, подобные TunnelVision, вполне могут быть использованы для нарушения конфиденциальности пользователей.