Как защитить корпоративные сети от атак и несанкционированного доступа.

Check Point Software Technologies Ltd. – это компания, специализирующаяся на разработке и поставке продуктов и решений в области кибербезопасности для защиты компьютерных сетей, серверов и мобильных устройств от различных видов киберугроз. Она является одним из лидеров в отрасли кибербезопасности.
 Компания предлагает решения для защиты от различных угроз, таких как вредоносные программы, хакерские атаки, кибершпионаж, атаки на приложения и многое другое." data-html="true" data-original-title="Check Point" >Check Point сообщила, что злоумышленники нацелены на устройства Check Point Remote Access VPN («Virtual Private Network» или «виртуальная частная сеть») — это совокупность технологий для создания одного или нескольких сетевых соединений (логической сети) поверх другой сети (например, Интернет). Технология создает виртуальный зашифрованный туннель между двумя серверами, представляя отправленные с устройства данные в виде случайной и зашифрованной строки кода. VPN также маскирует IP-адрес и местоположение пользователя в реальном времени для доступа к контенту без ограничений." data-html="true" data-original-title="VPN" >VPN в рамках продолжающейся кампании по взлому корпоративных сетей.

Удаленный доступ интегрирован во все сетевые межсетевые экраны Check Point. Его можно настроить как VPN «клиент-сеть» для доступа к корпоративным сетям через VPN-клиенты или настроить как SSL VPN для доступа через Интернет. Хакеры заинтересованы во внедрении в сети организаций через настройки удаленного доступа, чтобы, выискивая уязвимости, попытаться обнаружить активы предприятия и пользователей.

По данным Check Point, киберпреступники нацелены на шлюзы безопасности с устаревшими локальными учетными записями, использующие небезопасную аутентификацию только по паролю. Такая методика требует сочетания с аутентификацией по сертификату для предотвращения нарушений. Компания заявила, что к 24 мая выявила 3 попытки входа в систему, в том числе в системы различных поставщиков ИБ-решений и клиентов Check Point.

Чтобы защититься от продолжающихся атак, Check Point призвала клиентов проверять наличие уязвимых учетных записей в продуктах Quantum Security Gateway и CloudGuard Network Security, а также в программных блейдах Mobile Access и Remote Access VPN. Клиентам рекомендуется изменить метод аутентификации пользователя на более безопасные варианты или удалить уязвимые локальные учетные записи из базы данных Сервера управления безопасностью.

Компания также выпустила исправление Security Gateway, которое блокирует аутентификацию с помощью пароля для всех локальных учетных записей. После установки исправления локальные учетные записи со слабой проверкой подлинности не смогут войти в Remote Access VPN. Уязвимая локальная учетная запись будет заблокирована после установки исправления.

Уязвимая локальная учетная запись заблокирована после установки исправления

Клиенты могут найти дополнительную информацию об улучшении безопасности своих VPN в статье поддержки, где также приводятся рекомендации по реагированию на попытки несанкционированного доступа.

Check Point — не единственная компания, которая подверглась атаке на VPN-устройства за последние месяцы. В апреле международная кибербезопасность оказалась под угрозой после того, как эксперты из Cisco Talos обнаружили крупномасштабную кампанию по подбору учетных данных, нацеленную на VPN и SSH-сервисы устройств таких компаний, как Cisco, Check Point, Fortinet, SonicWall и Ubiquiti.

В конце марта 2024 года Cisco уже предупреждала о волне атак, направленных на службы удаленного VPN-доступа на устройствах Cisco Secure Firewall. Эти атаки особенно эффективны против слабых политик паролей, так как злоумышленники используют небольшой набор часто встречающихся паролей для множества имен пользователей.