Аннотация – В документе представлен подробный анализ угроз, возникающих при использовании небезопасных маршрутизаторов для малого офиса / домашнего офиса (SOHO). Анализ охватывает различные аспекты, включая проблемы безопасности и эксплойты, воздействие на критическую инфраструктуру.

В документе предлагается качественная сводка текущего состояния безопасности маршрутизаторов SOHO, в которой подчёркиваются риски, создаваемые небезопасными устройствами, и шаги, которые можно предпринять для снижения этих рисков. Анализ полезен специалистам по безопасности, производителям и различным отраслям промышленности, обеспечивая всестороннее понимание угроз и руководящих принципов повышения безопасности маршрутизаторов SOHO.

I. Введение

Эксплуатация небезопасных маршрутизаторов SOHO злоумышленниками, особенно группами, спонсируемыми государством, представляет значительную угрозу для отдельных пользователей и критически важной инфраструктуры. Производителям настоятельно рекомендуется применять принципы security by-design, privacy-by-design и методы повышения прозрачности для снижения этих рисков, в то время как пользователям и безопасникам рекомендуется внедрять передовые методы обеспечения безопасности маршрутизаторов и сохранять бдительность в отношении потенциальных угроз.

II. Проблема небезопасных маршрутизаторов SOHO

Причины небезопасных маршрутизаторов SOHO многогранны, включая как технические уязвимости, так и ошибки производителей в методах безопасного проектирования и разработки, а также небрежность пользователей при обеспечении безопасности маршрутизаторов.

.

- **Распространённые уязвимости**: Значительное количество уязвимостей, общее число которых составляет 226, было выявлено в популярных брендах маршрутизаторов SOHO. Эти уязвимости различаются по степени серьёзности, но в совокупности представляют существенную угрозу.
- **Устаревшие компоненты**: Основные компоненты, такие как ядро Linux, и дополнительные службы, такие как VPN, в этих маршрутизаторах устарели. Это делает их восприимчивыми к известным эксплойтам уязвимостей, которые уже давно стали достоянием общественности.
- **Небезопасные настройки по умолчанию**: Многие маршрутизаторы поставляются с простыми паролями по умолчанию и отсутствием шифрования соединений, чем пользуются злоумышленники.
- **Отсутствие security-by-design**: Маршрутизаторам SOHO часто не хватает ряда функций безопасности, например возможностей автоматического обновления и отсутствия эксплуатируемых проблем, особенно в интерфейсах веб-управления.
- **Доступность интерфейсов управления**: Производители часто создают устройства с интерфейсами управления, с доступом через Интернет по умолчанию, часто без уведомления клиентов об этой небезопасной конфигурации.
- **Отсутствие прозрачности и подотчётности**: производители не обеспечивают прозрачность путём раскрытия уязвимостей продукта с помощью программы CVE и точной классификации этих уязвимостей с использованием CWE
- **Пренебрежение безопасностью в пользу удобства и функциональных возможностей**: Производители отдают предпочтение простоте использования и широкому спектру функций, а не безопасности, что приводит к созданию маршрутизаторов, которые "недостаточно безопасны" прямо из коробки, без учёта возможности эксплуатации.
- **Небрежность пользователей**: Многие пользователи, включая ИТ-специалистов, не соблюдают базовые правила безопасности, такие как смена паролей по умолчанию или обновление встроенного программного обеспечения, оставляя маршрутизаторы уязвимыми для атак.
- **Сложность идентификации уязвимых устройств**: Идентификация конкретных уязвимых устройств является сложной из-за юридических и технических проблем, усложняющих процесс их устранения.

III. Сектора / Отрасли

Эксплуатация небезопасных маршрутизаторов SOHO представляет серьёзную угрозу во многих секторах, что подчёркивает необходимость улучшения методов обеспечения безопасности.

A. *Коммуникации*

- **Утечки данных и перехват данных**: небезопасные маршрутизаторы могут привести к несанкционированному доступу к сетевому трафику, позволяя злоумышленникам перехватывать конфиденциальные сообщения.
- **Нарушение работы служб**: скомпрометированные маршрутизаторы могут использоваться для запуска распределённых атак типа "Отказ в обслуживании" (DDoS), нарушающих работу служб связи.

B. *Транспорт и Логистика*

Уязвимость инфраструктуры: транспортный сектор в значительной степени полагается на сетевые системы для выполнения операций. Скомпрометированные маршрутизаторы могут позволить злоумышленникам нарушить работу систем управления трафиком и логистических операций.

C. *Водоснабжение*

Операционные технологии (OT): небезопасные маршрутизаторы предоставляют злоумышленникам шлюз для атак на системы OT в секторе водоснабжения, что потенциально влияет на системы очистки и распределения воды.

D. *Энергетика*

Сетевая безопасность: Энергетический сектор, особенно предприятия электроэнергетики, подвержены риску целенаправленных атак через небезопасные маршрутизаторы. Злоумышленники могли получить доступ к системам управления, создавая угрозу стабильности электросети.

E. *Другие отрасли*

- **Здравоохранение**: Небезопасные маршрутизаторы могут скомпрометировать данные пациентов и нарушить работу медицинских служб, предоставляя злоумышленникам доступ к сетям здравоохранения.
- **Розничная торговля и гостиничный бизнес**: Эти сектора уязвимы для утечки данных, связанных с информацией о клиентах и финансовыми транзакциями, из-за небезопасных сетевых устройств.
- **Промышленность**: Промышленные системы управления могут быть взломаны через небезопасные маршрутизаторы, что влияет на производственные линии и производственные процессы.
- **Образование**: Школы и университеты подвержены риску утечки данных и сбоев в предоставлении образовательных услуг.
- **Государственный и общественный сектор**: небезопасные маршрутизаторы могут привести к несанкционированному доступу к правительственным сетям, подвергая риску конфиденциальную информацию и критически важные услуги

IV. Основные выводы об использующих небезопасные маршрутизаторы SOHO

- **Эксплуатация группами, спонсируемыми государством**: Спонсируемая Китайской Народной Республикой (КНР) Volt Typhoon group активно компрометирует маршрутизаторы SOHO, используя проблемы ПО, который затем используются в качестве стартовых площадок для дальнейшей компрометации критически важных объектов инфраструктуры США.
- **Воздействие на критически важную инфраструктуру**: Взломанные маршрутизаторы SOHO представляют серьёзную угрозу, поскольку они могут использоваться для распространения внутри сетей и дальнейшего подрыва критически важных секторов инфраструктуры в США, включая связь, энергетику, транспорт и водоснабжение.
- **ZuoRAT Campaign**: Выявлена ZuoRAT кампания с использованием заражённых маршрутизаторов SOHO, где задействован троян, предоставляющий удалённый доступ и позволяющий сохранять незаметное присутствие в целевых сетях и для сбора конфиденциальную информацию.
- **Формирована ботнета**: скомпрометированные маршрутизаторы могут быть задействованы в ботнетах, крупных сетях заражённых устройств, используемых для запуска распределённых атак типа "отказ в обслуживании" (DDoS), кампаний рассылки спама и других вредоносных действий.
- **Атаки типа "MITM"**: использование уязвимости в маршрутизаторах для перехвата данных, проходящих по сети, и манипулирования ими, что приводит к утечке данных, краже личных данных и шпионажу.

A. *TTPs*

- **Вредоносное ПО KV Botnet**: Volt Typhoon внедрили вредоносное ПО KV Botnet в устаревшие маршрутизаторы Cisco и NETGEAR SOHO, которые больше не поддерживаются исправлениями безопасности или обновлениями ПО.
- **Сокрытие источника**: совершая действия через маршрутизаторы SOHO, возможно скрывать происхождение действий из КНР, что усложняет обнаружение и атрибуцию атак.
- **Нацеливание на электронные письма**: замечено, что Volt Typhoon нацеливались на электронные письма ключевых сетевых и ИТ-сотрудников, чтобы получить первоначальный доступ к сетям.
- **Использование мульти прокси-серверов**: для C2-инфраструктуры участники используют multi-hop

прокси-серверы, обычно состоящие из VPS или маршрутизаторов SOHO.

- **Методы LOTL**: вместо того, чтобы полагаться на вредоносное ПО для выполнения после компрометации, Volt Typhoon использовали встроенные инструменты и процессы в системах, стратегию, известную как LOTL, для закрепления и расширения доступа к сетям жертв.

B. Воздействие и ответные меры

- **Нарушение работы критически важной инфраструктуры**: Эксплуатация маршрутизаторов представляет значительную угрозу, поскольку потенциально может нарушить работу основных служб, предоставляемых секторами критически важной инфраструктуры.
- **Федеральный ответ**: ФБР и Министерство юстиции провели операции по нарушению работы ботнета KV путем удаленного удаления вредоносного ПО с заражённых маршрутизаторов и принятия мер по разрыву их соединения с ботнетом.
- **Компромиссный ответ**: Volt Typhoon продемонстрировал сложность защиты от госкампаний кибершпионажа и решающую роль сотрудничества между правительством, частным сектором и международными партнёрами. Подчёркивалась необходимость комплексных стратегий кибербезопасности, которые включают защиту устройств, обмен информацией об угрозах и информирование общественности. Поскольку киберугрозы продолжают развиваться, необходимы и коллективные усилия по защите критически важной инфраструктуры и поддержанию целостности глобальных сетей.
- **Государственно-частное партнёрство**: Компромиссные меры в ответ на Volt Typhoon предполагали тесное сотрудничество между правительственными учреждениями, включая ФБР и CISA, и организациями частного сектора. Это партнёрство способствовало обмену информацией об угрозах, техническими индикаторами компрометации (IoC) и передовыми практиками по смягчению последствий.
- **Анализ прошивки и исправление**: Производители затронутых маршрутизаторов SOHO были предупреждены об уязвимостях, используемых участниками Volt Typhoon. Были предприняты усилия по анализу вредоносного ПО, пониманию методов эксплуатации и разработке исправлений для устранения уязвимостей.
- **Меры по смягчению последствий**: ФБР уведомляет владельцев или операторов маршрутизаторов SOHO, доступ к которым был получен во время операции «по демонтажу». Меры по смягчению последствий, санкционированные судом, носят временный характер, и перезапуск маршрутизатора без надлежащего смягчения последствий сделает устройство уязвимым для повторного заражения.

C. Общественный и потребительский спрос на безопасность

В современную цифровую эпоху безопасность сетевых устройств стала первостепенной заботой как для населения, так и для бизнеса. Такая повышенная осведомлённость обусловлена растущим числом громких кибератак и утечек данных, которые подчеркнули уязвимости, присущие подключённым устройствам. В результате растёт спрос со стороны потребителей и общественности на то, чтобы производители уделяли приоритетное внимание безопасности в своих продуктах.

1) Факторы, определяющие спрос

- **Повышение осведомлённости о киберугрозах**: Широкая общественность и предприятия становятся все более осведомлёнными о рисках, связанных с киберугрозами, включая потенциальные финансовые потери, нарушения конфиденциальности и сбои в работе сервисов.
- **Давление со стороны регулирующих органов**: Правительства и регулирующие органы по всему миру внедряют более строгие правила и стандарты кибербезопасности, вынуждая производителей улучшать функции безопасности своих продуктов.
- **Экономические последствия кибератак**: Экономические последствия кибератак, включая стоимость восстановления и влияние на репутацию бренда, сделали безопасность критически важным фактором для покупателей при выборе продуктов.
- **Взаимосвязанность устройств**: Распространение устройств Интернета вещей и взаимосвязанность цифровых экосистем усилили потенциальное воздействие взломанных устройств, сделав безопасность приоритетом для обеспечения целостности личных и корпоративных данных.

2) Ожидания клиентов

- **Встроенные функции безопасности**: теперь клиенты ожидают, что устройства будут поставляться с надёжными встроенными функциями безопасности, которые защищают от широкого спектра угроз, не требуя обширных технических знаний для настройки.
- **Регулярные обновления системы безопасности**: ожидается, что производители будут предоставлять регулярные и своевременные обновления системы безопасности для устранения новых уязвимостей по мере их обнаружения.
- **Прозрачность**: Клиенты требуют от производителей прозрачности в отношении безопасности их продуктов, включая чёткую информацию об известных уязвимостях и шагах, предпринимаемых для их устранения.

- **Простота использования**: Клиенты, требующие высокого уровня безопасности, также ожидают, что эти функции будут удобными для пользователя и не повлияют на функциональность или производительность устройства.

D. Ответственность производителей

1) Основные элементы Secure by Design

- **Безопасность как основополагающее требование**: Безопасность следует рассматривать как основное требование, аналогичное функциональности, удобству использования и производительности на этапе всего жизненного цикла.
- **Минимизация поверхностей атаки**: Уменьшение количества потенциальных точек атаки внутри системы. Это предполагает ограничение функциональности и прав доступа системы только тем, что необходимо для ее функционирования, тем самым уменьшая возможности для эксплуатации.
- **Настройки безопасности по умолчанию**: Продукты должны поставляться с настройками безопасности по умолчанию, требующими от пользователей сознательного принятия решений по ослаблению безопасности. Это включает надёжные пароли по умолчанию, отключенные ненужные службы и включенное шифрование.
- **Принцип наименьших привилегий**: Обеспечение работы процессов, пользователей и систем с использованием минимального набора привилегий, необходимого для выполнения их задач. Это ограничивает потенциальный ущерб от эксплойта или взлома.
- **Безопасный отказ: проектирование** систем, обеспечивающих безопасный отказ в случае компрометации. Это означает, что когда система обнаруживает ошибку или нарушение, она по умолчанию переходит в состояние, которое минимизирует риск и подверженность.
- **Безопасность через прозрачность**: Поощрение открытости в отношении разработки и внедрения функций безопасности, обеспечение общественного контроля и экспертной оценки. Такая прозрачность помогает более эффективно выявлять и устранять уязвимости.
- **Privacy by Design**: интеграция Privacy by Design при разработке продукта, обеспечение защиты пользовательских данных и ответственного обращения с ними.
- **Оценка и управление рисками**: Проведение тщательной оценки рисков для понимания рисков безопасности, связанных с функциями и возможностями маршрутизатора, и управления ими.
- **Архитектура безопасности**: Разработка надёжной архитектуры безопасности, включающей аппаратные и программные компоненты, предназначенные для защиты от известных и возникающих угроз

2) Реализация в маршрутизаторах SOHO

- **Автоматические обновления**: Реализация механизмов автоматического обновления встроенного программного обеспечения для обеспечения того, чтобы на маршрутизаторах всегда работала последняя версия с самыми последними исправлениями безопасности. Это снижает зависимость от ручного обновления устройств.
- **Цифровая подпись**: Обеспечение цифровой подписи обновлений для проверки их подлинности и целостности. Это предотвращает установку вредоносных обновлений встроенного ПО, которые могут скомпрометировать маршрутизатор.
- **Безопасный веб-интерфейс управления**: Размещение веб-интерфейса управления на портах локальной сети и повышение его безопасности для обеспечения безопасного использования при доступе через Интернет. Это включает в себя внедрение надёжных механизмов аутентификации и шифрования.
- **Контроль доступа**: Ограничение доступа к веб-интерфейсу управления маршрутизатором со стороны локальной сети по умолчанию и предоставление опций для безопасного включения удалённого управления при необходимости.
- **Надёжные пароли по умолчанию**: Поставка маршрутизаторов с надёжными уникальными паролями по умолчанию для предотвращения несанкционированного доступа. Рекомендуется пользователям менять эти пароли во время первоначальной настройки.
- **Шифрование**: Использование шифрования для веб-интерфейса управления для защиты связи между маршрутизатором и пользователем.
- **Аутентификация**: Реализация механизмов надёжной аутентификации, включая возможность многофакторной аутентификации, для обеспечения доступа к интерфейсу управления маршрутизатором
- **Безопасные настройки по умолчанию**: маршрутизаторы по умолчанию поставляются с безопасными конфигурациями, такими как надёжные уникальные пароли, и отключены ненужные службы. Пользователей следует предостеречь от небезопасных конфигураций, если они решат переопределить значения по умолчанию.
- **Раскрытие уязвимостей и исправление**: Разработка четкой, ответственной политики раскрытия уязвимостей и своевременное предоставление исправлений. Это включает в себя

участие в программе CVE по отслеживанию и раскрытию уязвимостей.

- **Поддержка по окончании срока службы**: Решающее значение имеет чёткое информирование о политике по окончании срока службы (EOL) для продуктов и предоставление поддержки и обновлений на протяжении всего жизненного цикла продукта. Для устройств, которые больше не поддерживаются, производителям следует предоставить рекомендации по безопасной утилизации или замене.

3) Последствия для производителей

- **Баланс между безопасностью и удобством использования**: Одной из проблем при реализации принципов Secure by Design является поддержание удобства использования. Меры безопасности не должны чрезмерно усложнять работу пользователя.
- **Финансовые издержки**: Разработка безопасных продуктов может повлечь за собой дополнительные расходы. Однако долгосрочные выгоды от снижения риска взломов и атак оправдывают эти инвестиции.
- **Непрерывное развитие**: Обеспечение безопасности — это не разовое мероприятие, оно требует постоянного внимания для адаптации к новым угрозам и уязвимостям.
- **Укрепление доверия**: Уделяя приоритетное внимание безопасности, производители получают возможность укреплять доверие клиентов, продукцию на конкурентном рынке.
- **Глобальная цепочка поставок**: Маршрутизаторы SOHO часто производятся как часть сложной глобальной цепочки поставок. Обеспечение безопасности по всей этой цепочке, от производителей компонентов до окончательной сборки, требует координации и соблюдения передовых методов обеспечения безопасности на каждом этапе.

V. Последствия атак на маршрутизаторы

- **Распространённые уязвимости**: Значительное количество уязвимостей, всего около 226 в совокупности представляют существенную угрозу безопасности.
- **Устаревшие компоненты**: Основные компоненты, такие как ядро Linux, и дополнительные службы, такие как VPN, устарели, что делает их уязвимыми для известных эксплойтов.
- **Пароли по умолчанию и незашифрованные соединения**: Многие маршрутизаторы поставляются с легко угадываемыми паролями по умолчанию и используют незашифрованные соединения, которыми могут легко воспользоваться злоумышленники.
- **Скомпрометированные устройства и данные**: После взлома маршрутизатора все устройства, защищенные его брандмауэром, становятся уязвимыми, позволяя злоумышленникам отслеживать, перенаправлять, блокировать или изменять данные.
- **Риск для критической инфраструктуры**: скомпрометированные маршрутизаторы SOHO могут использоваться для атаки на критическую инфраструктуру США, потенциально нарушая работу основных служб в секторах связи, энергетики, транспорта и водоснабжения.
- **Отказ в обслуживании и перехват трафика**: Уязвимости в протоколах могут приводить к атакам типа "отказ в обслуживании" против служб хоста и перехвату как внутреннего, так и внешнего трафика.
- **Перехват и кибератаки**: Злоумышленники могут перехватывать трафик и запускать дальнейшие сетевые атаки, затрудняя пользователям обнаружение взлома из-за минимальных пользовательских интерфейсов маршрутизатора.
- **Отсутствие методов обеспечения безопасности**: Исследования показывают, что многие пользователи, включая ИТ-специалистов, не соблюдают базовые методы обеспечения безопасности, такие как смена паролей по умолчанию или обновление встроенного программного обеспечения, что делает маршрутизаторы уязвимыми для атак.
- **Потенциал для широкомасштабной эксплуатации**: Само количество уязвимых устройств, исчисляемое миллионами, указывает на значительный потенциал для широкомасштабной эксплуатации злоумышленниками.
- **Юридические и технические проблемы**: Идентификация конкретных уязвимых устройств является сложной задачей из-за юридических и технических проблем, что усложняет процесс устранения этих уязвимостей.
- **Повышенная осведомлённость, но постоянные риски**: несмотря на растущую осведомлённость и усилия по повышению безопасности маршрутизаторов SOHO, многие известные недостатки остаются не устраненными, а продолжают обнаруживаться новые уязвимости