RFC 4272 — Анализ уязвимостей протокола BGP

Статус документа

В этом документе содержится спецификация протокола, предложенного сообществу Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации протокола вы можете узнать из документа "Internet Official Protocol Standards" (STD 1). Документ может распространяться без ограничений.

Тезисы

Протокол BGP-4 (Border Gateway Protocol v4), как и множество других протоколов разработанных до того, как среда Internet стала зоной риска, создавался без принятия существенных мер по защите передаваемой информации. Внутри протокола BGP отсутствуют механизмы защиты от атак, которые изменяют, удаляют, подменяют или воспроизводят перехваченные данные и могут вносить существенные помехи в работу системы маршрутизации.
В этом документе обсуждаются некоторые вопросы безопасности, связанные с распространением маршрутной информации BGP. Документ не рассматривает вопросов безопасности при пересылке пакетов.

Оглавление

1. Введение

Протокол междоменной маршрутизации BGP был создан, когда среда Internet еще не стала столь паскудной, какой она является сегодня. В результате архитектура BGP не включает средств

защиты от случайных или обдуманных атак, которые могли бы повредить работе системы маршрутизации Internet.
В этом документе рассматриваются уязвимости протокола BGP, соответствующего спецификации [RFC4271]. Предполагается, что читатель знаком с документами RFC, посвященными протоколу BGP и поведению BGP-систем.
Очевидно, что сеть Internet уязвима для атак с использованием протоколов маршрутизации и BGP в этом смысле не является исключением. Дефектные, некорректно настроенные или преднамеренно искаженные источники могут внести существенные искажения в работу Internet путем вставки ложной маршрутной информации в распространяемые с помощью BGP базы маршрутных данных (путем изменения, подмены или повторного использования пакетов BGP). Существуют также некоторые методы нарушения работы сети в целом путем разрыва связей в системе обмена информацией между узлами BGP. Источниками ложной информации могут служить как внешние хосты (outsider) так и легитимные узлы BGP.
Криптографическая аутентификация обмена данными между партнерами не предусмотрена в BGP. Как и стек TCP/IP, протокол BGP может служить целью всех атак, включая IP spoofing, захват сессий и т. п. Любой сторонний узел может включить правдоподобные сообщения BGP в обмен данными между партнерами BGP и, следовательно, включить в таблицы обманные маршруты или разорвать соединение между партнерами. Любое прерывание связи между партнерами приводит к изменению распространяемой картины маршрутизации. Более того, внешние узлы могут также разрывать соединения между партнерами BGP, обрывая для них сессии TCP с помощью обманных пакетов. Внешние источники обманной информации BGP могут располагаться в любой точке сети Internet.
Вследствие перечисленных выше проблем текущая спецификация BGP требует от реализаций протокола BGP поддержки механизма аутентификации, описанного в документе [TCPMD5]. Однако требование поддержки механизма аутентификации еще не означает его использования на практике. Механизм [TCPMD5] основан на использовании предустановленного разделяемого секрета (shared secret) и не включает возможностей IPsec [IPsec] по динамическому согласованию этого секрета. Следовательно, использование [TCPMD5] должно быть осознанным решением и не может быть включено автоматически или по умолчанию.
Текущая спецификация BGP также позволяет реализациям протокола принимать соединения от неуказанных в конфигурации партнеров ([RFC4271], глава 8). Однако в спецификации отсутствует четкое определение «неуказанного в конфигурации партнера» или способов использования аутентификации [TCPMD5] для таких случаев. Следовательно, анализ данного аспекта безопасности не представляется возможным. Когда будет выпущена спецификация, полностью описывающая эту проблему, анализ безопасности должен стать частью этой спецификации.
Сами узлы BGP могут включать ложные маршрутные данные, маскируясь под другой легитимный узел BGP или рассылая маршрутную информацию от своего имени без должных на то полномочий. Наблюдались случаи, когда некорректно настроенные или неисправные маршрутизаторы становились причиной серьезных нарушений в работе Internet. Легитимные узлы BGP имеют контекст и информацию для создания правдоподобных, но ложных маршрутных данных, и, следовательно, могут служить причиной серьезных нарушений. Криптографическая защита [TCPMD5] и защита работающих устройств не позволяют исключить ложную информацию, полученную от легитимного партнера. Риск нарушений, вызываемых легитимными партнерами BGP, является реальным и должен приниматься во внимание.
Ложные маршрутные данные могут оказывать различное влияние на картину маршрутизации. Если ложные данные удаляют корректную маршрутную информацию для отдельной сети, эта сеть может стать недоступной для части Internet, принявшей ложные данные. Если ложная информация изменяет маршрут в сеть, пакеты, адресованные в эту сеть, могут пересылаться по неоптимальному пути, путь пересылки не будет соответствовать ожидаемой политике или трафик будет просто утерян. В результате трафик в эту сеть может быть задержан на пути, который будет длиннее необходимого. Сеть может стать недоступной для областей, принявших ложные данные. Трафик может быть также направлен по пути, на котором данные могут быть подвергнуты нежелательному просмотру или искажены. Если ложная информация показывает, что автономная система включает сети, которые реально в нее не входят, пакеты для таких сетей могут быть не доставлены из тех частей Internet, которые приняли ложную информацию. Ложные анонсы принадлежности сетей к автономной системе могут также привести к фрагментированию агрегированных адресных блоков в других частях Internet и вызвать проблемы в маршрутизации для других сетей.
К нарушениям в результате таких атак относятся:

- starvation (потеря пакетов)
- Трафик, адресованный узлу, пересылается в ту часть сети, которая не может обеспечить его доставку;
- network congestion (перегрузка сети)

- Через какую-либо часть сети будет пересылаться больше данных, нежели эта сеть способна обработать;
- blackhole (черная дыра)
- Большое количество трафика направляется для пересылки через один маршрутизатор, который не способен справиться с возросшим уровнем трафика и будет отбрасывать часть, большинство или все пакеты;
- delay (задержка)
- Данные, адресованные узлу, пересылаются по более длинному пути, чем обычно;
- looping (петли)
- Данные передаются по замкнутому пути и никогда не будут доставлены;
- eavesdrop (перехват)
- Данные пересылаются через какой-либо маршрутизатор или сеть, которые не должны видеть эти данные, информация при такой пересылке может просматриваться;
- partition (разделение сети)
- Некоторые части кажутся отделенными от сети, хотя на самом деле это не так;
- cut (отключение)
- Некоторые части сети могут казаться отрезанными от сети, хотя реально они подключены;
- churn (волны)
- Скорость пересылки в сеть изменяется быстрыми темпами, что приводит к значительным вариациям картины доставки пакетов (и может неблагоприятно влиять на работу системы контроля насыщения);
- instability (нестабильность)
- Работа BGP становится нестабильной и не удается достичь схождения картины маршрутов;
- overload (перегрузка)
- Сообщения BGP сами по себе становятся значительной частью передаваемого через сеть трафика;
- resource exhaustion (истощение ресурсов)
- Сообщения BGP сами по себе отнимают слишком много ресурсов маршрутизатора (например, пространства таблиц);
- address-spoofing (обманные адреса)
- Данные пересылаются через некий маршрутизатор или сеть, которые являются подставными и могут служить для перехвата или искажения информации.

1.1. Уровни требований

Ключевые слова необходимо (MUST), недопустимо (MUST NOT), требуется (REQUIRED), нужно (SHALL), не нужно (SHALL NOT), следует (SHOULD), не следует (SHOULD NOT), рекомендуется (RECOMMENDED), возможно (MAY), необязательно (OPTIONAL) в данном документе интерпретируются в соответствии с RFC 2119 [RFC2119].

2. Атаки

Протокол BGP, как таковой, подвержен перечисленным ниже типам атак (список получен на основе IAB RFC с рекомендациями по подготовке разделов "Вопросы безопасности" для RFC [SecCons]).

- confidentiality violations (нарушение конфиденциальности)
- Маршрутные данные BGP передаются в открытом текстовом виде, что позволяет легко перехватывать информацию (конфиденциальность маршрутных данных не является общим требованием).
- replay (воспроизведение)
- BGP не включает мер по предотвращению повторного использования перехваченных сообщений.
- message insertion (вставка сообщений)
- BGP не включает защиты от вставки сообщений. Однако, поскольку BGP использует транспорт TCP, при завершенной организации соединения вставка сообщений внешним узлом потребует точного предсказания порядковых номеров (такое предсказание возможно, но весьма затруднено для хороших реализаций TCP) или перехвата сессий.
- message deletion (удаление сообщений)
- BGP не включает защиты от удаления сообщений. Опять-таки, такие атаки весьма затруднены для качественных реализаций TCP, но исключить их полностью нельзя.
- message modification (изменение сообщений)

- BGP не включает защиты от изменения сообщений. Синтаксически корректная модификация без изменением размера данных TCP в общем случае будет незаметной.
- Man-in-the-middle (атаки с участием человека)
- BGP не включает средств защиты от MITM-атак. BGP не использует аутентификации партнеров и такие атаки становятся «детской игрушкой».
- denial of service (атаки на службы)
- Хотя ложные маршрутные данные сами по себе могут служить DoS-атакой на конечную систему, пытающуюся передавать данные через сеть, и сеть в целом, некоторые виды ложной информации могут создавать DoS-атаки на сам протокол BGP. Например, анонсирование большого числа более специфичных маршрутов (более длинных префиксов) может привести к росту трафика BGP и размера таблиц маршрутизации, который окажется неприемлемым для системы.

Обязательная поддержка механизма [TCPMD5] будет предотвращать вставку, удаление и изменение сообщений, а также MITM- и DoS-атаки со стороны внешних узлов. Использование [TCPMD5] не защищает от перехвата, но обеспечение конфиденциальности данных не входит в задачи протокола BGP. Механизм [TCPMD5] не обеспечивает зашиты от replay-атак и против них единственным средством защиты являются порядковые номера TCP. Следовательно, возможность организации таких атак на соединения BGP сохраняется и при использовании [TCPMD5], но только в течение очень короткого времени. Механизм [TCPMD5] не обеспечивает защиты от ложных маршрутных данных, распространяемых внутренним источником (insider).

3. Уязвимости и риски

Связанные с протоколом BGP риски обусловлены тремя основными уязвимостями:

1. BGP не имеет внутреннего механизма обеспечения сильной защиты целостности и актуальности данных, а также аутентификации партнеров для сообщений, передаваемых между узлами BGP.
2. Отсутствует механизм проверки полномочий AS для анонсируемой информации NLRI.
3. Отсутствует механизм обеспечения достоверности атрибутов пути, анонсируемых AS.

Первая из перечисленных уязвимостей закрывается обязательной поддержкой [TCPMD5] в спецификации BGP. После развертывания [TCPMD5] целостность сообщения и аутентификация партнеров будут обеспечены. Механизм [TCPMD5] предполагает, что алгоритм MD5 является безопасным, а разделяемый секрет защищен и достаточно сложно предсказуем.
В последующем обсуждении уязвимости будут описываться в терминах машины конечных состояний BGP FSM. Указанные здесь события определены и обсуждаются в разделе 8 документа [RFC4271]. К таким событиям относятся:

- [Административные события]
- Событие 2: ManualStop
- Событие 8: AutomaticStop
- [Таймеры]
- Событие 9: ConnectRetryTimer_Expires
- Событие 10: HoldTimer_Expires
- Событие 11: KeepaliveTimer_Expires
- Событие 12: DelayOpenTimer_Expires
- Событие 13: IdleHoldTimer_Expires
- [События, связанные с соединениями TCP]
- Событие 14: TcpConnection_Valid
- Событие 16: Tcp_CR_Acked
- Событие 17: TcpConnectionConfirmed
- Событие 18: TcpConnectionFails
- [События, связанные с сообщениями BGP]
- Событие 19: BGPOpen
- Событие 20: BGPOpen with DelayOpenTimer running
- Событие 21: BGPHeaderErr
- Событие 22: BGPOpenMsgErr
- Событие 23: OpenCollisionDump
- Событие 24: NotifMsgVerErr
- Событие 25: NotifMsg
- Событие 26: KeepAliveMsg
- Событие 27: UpdateMsg
- Событие 28: UpdateMsgErr

3.1. Уязвимости в сообщениях BGP

Существует 4 типа сообщений BGP — OPEN, KEEPALIVE, NOTIFICATION и UPDATE. В этом разделе обсуждаются уязвимости, связанные с каждым типом сообщений и возможности внешних атакующих или узлов BGP по использованию этих уязвимостей. Внешние атакующие могут использовать ложные сообщения OPEN, KEEPALIVE, NOTIFICATION или UPDATE для нарушения соединений между партнерами BGP. Они могут также использовать сообщения UPDATE для нарушения маршрутизации без разрыва соединений между партнерами. Внешний атакующий может также нарушить связь между партнерами путем вставки ложных пакетов TCP, которые нарушат обработку соединений TCP. В общем случае возможности внешних атакующих по использованию ложных сообщений BGP и TCP ограничены (но не предотвращаются полностью), благодаря обработке порядковых номеров TCP. Использование [TCPMD5] будет дополнительным отражением таких атак. Партнеры BGP могут сами разрывать соединения между собой в любой момент, используя для этого сообщения NOTIFICATION. Таким образом, использование сообщений OPEN, KEEPALIVE или UPDATE не порождает дополнительного риска. Однако партнеры BGP могут нарушить картину маршрутизации (вполне реально), используя сообщения UPDATE, содержащие ложную маршрутную информацию. В частности, ложные атрибуты ATOMIC_AGGREGATE, NEXT_HOP и AS_PATH, а также некорректное значение NLRI в сообщениях UPDATE могут нарушить маршрутизацию. Использование [TCPMD5] не препятствует этому типу атак со стороны узлов BGP. Каждый тип сообщений связан с уязвимостями и риском, которые обсуждаются в следующих параграфах.

3.1.1. Заголовок сообщения

Событие 21. Каждое сообщение BGP начинается стандартным заголовком. Во всех случаях синтаксические ошибки в заголовке сообщения будут заставлять узел BGP закрывать соединение, освобождать все выделенные для BGP ресурсы, удалять все маршруты, полученные через это соединение, запускать процесс принятия решений для установки новой картины маршрутов и возвращаться в состояние Idle. В зависимости от реализации может также выполняться операция подавления «колебаний партнера». Этот процесс может влиять на время, через которое будет восстанавливаться разорванное соединение с партнером. Внешний атакующий, способный подменять сообщения, включая в них ошибки заголовков, может вызвать широкомасштабное нарушение картины маршрутизации.

3.1.2. OPEN

Событие 19. Прием сообщения OPEN узлом BGP, находящимся в состоянии Connect или Active будет заставлять узел закрыть соединение, освободить все связанные с ним ресурсы BGP, удалить связанные с соединением маршруты, запустить процесс принятия решения и перейти в состояние Idle. Удаление маршрутов приводит к каскадному эффекту, при котором изменения маршрутов распространяются через другие узлы. В зависимости от реализации может выполняться «подавление колебаний». Этот процесс может влиять на время, через которое будет восстанавливаться разорванное соединение с партнером.
В состоянии OpenConfirm или Established доставка сообщения OPEN может указывать на конфликт в соединении. Если данное соединение отбрасывается, вводится Событие 23 (это событие рассматривается ниже и может приводить к таким же нарушениям картины маршрутизации, какие указаны выше для состояний Connect и Active).
В состоянии OpenSent получение сообщения OPEN будет переводить узел BGP в состояние OpenConfirm. Если внешний узел может передавать ложные сообщения OPEN (для этого требуется очень точная синхронизация), более поздняя доставка сообщения OPEN от легитимного партнера может заставить узел BGP декларировать конфликт в соединении. Процедура детектирования конфликтов может привести к отказу от легитимного соединения.
В результате возможность внешнего атакующего подменять сообщения этого типа может приводить к существенному и широкомасштабному нарушению картины маршрутизации.
Событие 20. Если сообщение OPEN принято при запущенном таймере OpenDelay когда соединение находится в состоянии OpenSent, OpenConfirm или Established, узел BGP будет разрывать соединение, освобождать связанные с ним ресурсы BGP, удалять все связанные с соединением маршруты, запускать процесс принятия решений и переходить в состояние Idle. Удаление маршрутов может вызывать каскадный эффект, при котором изменения маршрутов распространяются через другие узлы. В зависимости от реализации может выполняться «подавление колебаний». Этот процесс может влиять на время, через которое будет восстанавливаться разорванное соединение с партнером. Поскольку таймер OpenDelay не должен

запускаться в перечисленных выше состояниях, описываемый эффект может быть вызван лишь ошибкой в реализации (передается сообщение NOTIFICATION с кодом ошибки "Finite State Machine Error"). Для внешнего атакующего весьма сложно (или невозможно) вызвать такую ошибку FSM.
В состояниях Connect и Active это событие будет приводить к переходу в состояние OpenConfirm. Как и для события 19, если внешний атакующий способен передавать подставные сообщения OPEN, которые будут приниматься при запущенном таймере DelayOpen, последующее прибытие сообщения OPEN (от легитимного партнера) может рассматриваться как конфликт в соединении с отказом от легитимного соединения.
Возможность внешнего атакующего подменять сообщения этого типа может приводить существенному и широкомасштабному нарушению картины маршрутизации.
Событие 22. Ошибки в сообщениях OPEN (например, недопустимое состояние Hold, некорректно сформированное поле Optional Parameter, неподдерживаемая версия и т. п.) будут заставлять узел BGP разрывать соединение, освобождать связанные с ним ресурсы BGP, удалять все связанные с соединением маршруты, запускать процесс принятия решений и переходить в состояние Idle. Удаление маршрутов может вызывать каскадный эффект, при котором изменения маршрутов распространяются через другие узлы. В зависимости от реализации может выполняться «подавление колебаний». Этот процесс может влиять на время, через которое будет восстанавливаться разорванное соединение с партнером. Следовательно, способность внешнего атакующего передавать обманные сообщения этого типа может приводить к существенным, широкомасштабным нарушениям картины маршрутизации.

3.1.3. KEEPALIVE

Событие 26. Прием сообщения KEEPALIVE в состоянии Connect, Active или OpenSent будет заставлять узел BGP переходить в состояние Idle и отказываться от организации соединения. В зависимости от реализации может выполняться «подавление колебаний». Этот процесс может влиять на время, через которое будет восстанавливаться разорванное соединение с партнером. Возможность внешнего атакующего передавать подставные сообщения этого типа может вести к нарушению картины маршрутизации. Для осознанного использования этой уязвимости сообщение KEEPALIVE должно быть аккуратно синхронизировано в последовательности сообщений, передаваемых между партнерами. При отсутствии такой синхронизации нарушения картины маршрутизации не произойдет.

3.1.4. NOTIFICATION

Событие 25. Прием сообщения NOTIFICATION в любом состоянии будет заставлять узел BGP разрывать соединение, освобождать связанные с ним ресурсы BGP, удалять все связанные с соединением маршруты, запускать процесс принятия решений и переходить в состояние Idle. Удаление маршрутов может вызывать каскадный эффект, при котором изменения маршрутов распространяются через другие узлы. Кроме того, в состоянии Established в зависимости от реализации может выполняться «подавление колебаний». Этот процесс может влиять на время, через которое будет восстанавливаться разорванное соединение с партнером. Следовательно, способность внешнего атакующего передавать обманные сообщения этого типа может приводить к существенным, широкомасштабным нарушениям картины маршрутизации.
Событие 24. Сообщение NOTIFICATION, содержащее код ошибки "Version Error" вызывает такой же эффект, как событие 25 с тем лишь отличием, что дополнительная операция «подавления колебаний» не выполняется в состояниях OpenSent и OpenConfirm или в состояниях Connect и Active с запущенным таймером DelayOpen. Следовательно, уровень возможных нарушений будет меньше, поскольку не оказывается воздействия на время восстановления соединения.

3.1.5. UPDATE

Событие 8. Узел BGP может по своему разумению разрывать соединение BGP, если общее число префиксов превышает заданное конфигурационными параметрами значение. В таких случаях сообщение UPDATE может содержать число префиксов, приводящее к превышению заданного порога. Узел BGP будет разрывать соединение, освобождать связанные с ним ресурсы BGP, удалять все связанные с соединением маршруты, запускать процесс принятия решений и переходить в состояние Idle. Удаление маршрутов может вызывать каскадный эффект, при котором изменения маршрутов распространяются через другие узлы. Кроме того, в состоянии Established в зависимости от реализации может выполняться «подавление колебаний». Этот процесс может влиять на время, через которое будет восстанавливаться разорванное соединение

с партнером. Следовательно, способность внешнего атакующего передавать обманные сообщения этого типа может приводить к существенным, широкомасштабным нарушениям картины маршрутизации.
Событие 28. Если сообщение UPDATE имеет некорректный формат, узел BGP будет разрывать соединение, освобождать связанные с ним ресурсы BGP, удалять все связанные с соединением маршруты, запускать процесс принятия решений и переходить в состояние Idle (некорректность формата может быть связана с неверными значениями полей Withdrawn Routes Length, Total Attribute Length или Attribute Length, отсутствием обязательных атрибутов, значением поля Attribute Flags, конфликтующим с Attribute Type Codes, синтаксическими ошибками в ORIGIN, NEXT_HOP или AS_PATH и т. п.). Удаление маршрутов может вызывать каскадный эффект, при котором изменения маршрутов распространяются через другие узлы. Кроме того, в состоянии Established в зависимости от реализации может выполняться «подавление колебаний». Этот процесс может влиять на время, через которое будет восстанавливаться разорванное соединение с партнером. Следовательно, способность внешнего атакующего передавать обманные сообщения этого типа может приводить к существенным, широкомасштабным нарушениям картины маршрутизации. Когда узел BGP имеет полномочия закрывать соединения по своему усмотрению, этот тип сообщений приводит к дополнительной возможности нарушения картины маршрутизации.
Событие 27. Сообщение UPDATE, полученное в любом состоянии за исключением Established, будет заставлять узел BGP разрывать соединение, освобождать связанные с ним ресурсы BGP, удалять все связанные с соединением маршруты, запускать процесс принятия решений и переходить в состояние Idle. Удаление маршрутов может вызывать каскадный эффект, при котором изменения маршрутов распространяются через другие узлы. Кроме того, в состоянии Established в зависимости от реализации может выполняться «подавление колебаний». Этот процесс может влиять на время, через которое будет восстанавливаться разорванное соединение с партнером. Следовательно, способность внешнего атакующего передавать обманные сообщения этого типа может приводить к существенным, широкомасштабным нарушениям картины маршрутизации.
В состоянии Established сообщения UPDATE служат для передачи маршрутной информации. Возможность подмены любой части сообщения этого типа, может вести к нарушению картины маршрутизации независимо от того, является источник сообщений внешним атакующим или легитимным узлом BGP.

3.1.5.1. Недопустимые значения Routes Length и Total Path Attribute Length

Существуют уязвимости, связанные с возможностью изменения значений этих полей. При изменении размера корректный разбор сообщения может стать невозможным, что приведет к возникновению ошибки, передаче сообщения NOTIFICATION и разрыву соединения (см. Событие 28, описанное выше). Поскольку корректно настроенный узел BGP имеет возможность в любое время разорвать соединение, эта уязвимость ведет к дополнительному риску только в тех случаях, когда источником является не указанный в конфигурации партнер BGP (т. е., не возникает дополнительного риска со стороны действующих партнеров BGP).

3.1.5.2. Поле WITHDRAWN ROUTES (отозванные маршруты)

Внешний атакующий может уничтожить корректные маршруты путем подмены этого поля. Атакующий может также уничтожить воссозданные (reestablished) маршруты, заново передавая данные об отзыве маршрутов из перехваченных ранее пакетов.
Узел BGP может «ошибочно» отозвать действующие маршруты, используя поле WITHDRAWN ROUTES. Однако, поскольку узел BGP имеет полномочия для всех анонсируемых им маршрутов, он вправе отзывать любые из анонсированных ранее маршрутов. В силу того, что принимающий узел BGP будет реально отзывать только маршруты, связанные с передающим отзыв маршрутов узлом BGP, не возникает возможности отзыва чужих маршрутов. Следовательно, здесь не возникает дополнительного риска со стороны партнеров BGP.

3.1.5.3. Атрибуты пути

С атрибутами пути связано множество уязвимостей и рисков.

- Attribute Flag, Attribute Type Code, Attribute Length
  Партнер BGP или внешний атакующий может изменить размер или тип (флаги или код типа) атрибута так, чтобы они не соответствовали значению атрибута. При изменении флагов эти флаги и код типа могут стать несовместимыми (например, обязательный атрибут будет указан как частный — partial), дополнительный атрибут может быть

интерпретирован как обязательный и наоборот. При изменении кода типа атрибут может быть интерпретирован как тип и значение иного атрибута.
Наиболее очевидным результатом изменения размера, флагов или кода будет ошибка при анализе сообщения UPDATE. Такая ошибка вызовет передачу сообщения NOTIFICATION с последующим разрывом соединения (см. описанное выше событие 28). Поскольку корректно настроенный узел BGP может в любой момент разорвать соединение, эта уязвимость приводит к дополнительному риску только в тех случаях, когда источником является внешний атакующий (т. е., не возникает дополнительного риска со стороны партнеров BGP).

- ORIGIN
  Это поле показывает источник маршрутной информации — IGP или EGP. Поле используется на этапе выбора маршрутов, следовательно, здесь имеется незначительная уязвимость, которая позволяет воздействовать на процесс выбора маршрутов принимающим узлом BGP путем изменения этого поля.
- AS_PATH
  Партнер BGP или внешний атакующий могут анонсировать значение AS_PATH, не связанное должным образом с NLRI.
  Поскольку партнер BGP может не проверять, что полученное значение AS_PATH начинается с номера AS его партнера, злонамеренный партнер BGP может анонсировать путь, начинающийся с номера AS любого узла BGP с минимальным воздействием на самого себя. Это может повлиять на процесс выбора маршрутов принимающим сообщение узлом BGP. Злонамеренный партнер может указать существенно более короткое значение AS_PATH, которое будет повышать шансы на выбор данного маршрута и, возможно, давать злонамеренному партнеру доступ к трафику, который он обычно не получает. Кратчайшее значение AS_PATH может также приводить к возникновению маршрутных петель, если в нем не содержится информации, требуемой для предотвращения петель.
  Узел BGP может быть настроен так, чтобы он принимал маршруты с номером своей AS в пути. Такие эксплуатационные вопросы определены как «выходящие за пределы» спецификации BGP. Но, поскольку AS_PATH может включать петли, разработчики не имеют возможности автоматически отбрасывать маршруты с петлями. Каждый узел BGP проверяет лишь отсутствие своего номера AS в AS_PATH.
  Вкупе с возможностью использования любых значений NEXT_HOP, это дает злонамеренным узлам BGP значительные возможности управления путями передачи трафика.
- Originating Routes
  Специальным случаем анонсирования ложных атрибутов AS_PATH является ситуация, когда AS_PATH анонсирует прямое подключение к указанной сети. Партнер BGP или внешний атакующий могут нарушить маршрутизацию в сеть (сети), указанную в поле NLRI, путем рассылки ложных анонсов прямого соединения с сетью. NLRI станет недоступным для части сети, которая воспримет этот ложный маршрут, пока последняя AS из AS_PATH не создаст туннель для пересылаемых пакетов этого NLRI в направлении целевой AS по корректному пути. Но даже после туннелирования пакетов в корректную AS маршрут может быть неоптимальным или несоответствующим заданной политике. Кроме того, может быть оказано воздействие на маршрутизацию для других сетей в Internet, если ложные анонсы фрагментируют агрегированный блок адресов, заставляя маршрутизаторы обрабатывать (передавать сообщения UPDATE, сохранять и поддерживать маршруты) множество фрагментов взамен одного агрегированного маршрута. Фальшивые исходные точки для множества адресов могут приводить к тому, что маршрутизаторы и транзитные сети на анонсированном пути начнут лавинную рассылку потерявшего направление трафика.
- NEXT_HOP
  Атрибут NEXT_HOP определяет IP-адрес граничного маршрутизатора, который следует использовать как следующий интервал при пересылке пакетов NLRI, указанному в сообщении UPDATE. Если получателем является внешний партнер, адрес получателя и значение NEXT_HOP должны находиться в одной подсети. Очевидно, что внешний атакующий, который изменит это поле, сможет нарушить пересылку трафика между двумя AS.
  Если получатель сообщения является внешним партнером AS и маршрут был получен от другой партнерской AS (это один из двух вариантов "third party" NEXT_HOP), тогда узел BGP, анонсирующий маршрут, имеет возможность направить трафик получателя узлу BGP, указанному адресом NEXT_HOP. Это дает возможность направить трафик на маршрутизатор, который не способен продолжать дальнейшую пересылку трафика. Злонамеренный узел BGP также может воспользоваться этим методом для того, чтобы заставить другую AS передавать трафик, который обычно через нее не проходит. В

некоторых случаях это может дать злонамеренному узлу BGP преимущества, поскольку он способен направить передачу трафика по более длинному пути в ту или иную точку, которую он разделяет с атакуемым.

- MULTI_EXIT_DISC
  Атрибут MULTI_EXIT_DISC используется в сообщениях UPDATE, передаваемых между партнерами, которые находятся в разных AS. Хотя полученное из другой AS значение MULTI_EXIT_DISC может распространяться внутри AS, его нельзя распространять в другие AS. В результате это поле используется только при внутреннем выборе маршрутов для одной AS. Изменение этого поля внешним атакующим или партнером BGP может сделать неоптимальной маршрутизацию внутри AS.
- LOCAL_PREF
  Атрибут LOCAL_PREF должен включаться во все сообщения для внутренних партнеров и исключаться из сообщений для внешних партнеров. Следовательно, изменение LOCAL_PREF может повлиять только на маршрутизацию внутри AS. Отметим, что в спецификации BGP отсутствует требование согласованности LOCAL_PREF между внутренними узлами BGP одной AS. Поскольку узлы BGP свободны в выборе значения LOCAL_PREF, изменение этого поля является уязвимостью только со стороны внешних атакующих.
- ATOMIC_AGGREGATE
  Поле ATOMIC_AGGREGATE показывает, что некая AS на пути объединяет несколько маршрутов и анонсирует объединенное значение NLRI без формирования AS_SET, обычно формируемого из AS в AS_PATH агрегированных маршрутов. Узлы BGP, получающие маршрут с ATOMIC_AGGREGATE, не могут делать NLRI более специфичным. Удаление атрибута ATOMIC_AGGREGATE снимает это ограничение и может стать причиной некорректной маршрутизации трафика, предназначенного для более специфичного NLRI. Добавление атрибута ATOMIC_AGGREGATE при отсутствии агрегирования будет давать незначительный эффект за счет того, что неагрегированный NLRI нельзя будет сделать более специфичным. Эта уязвимость существует независимо от того, является источник партнером BGP или внешним атакующим.
- AGGREGATOR
  Это поле может включаться узлом BGP, который создал маршруты, представленные в сообщении UPDATE, путем объединения других маршрутов. Поле содержит номер AS и IP-адрес последнего сумматора (aggregator) маршрута. Если поле не используется при выборе маршрутов, никакой уязвимости не возникает.

3.1.5.4. NLRI

Изменяя это поле, внешний атакующий или партнер BGP могут нарушить маршрутизацию для анонсируемой сети перегрузить маршрутизатор на анонсируемом пути, вызвать потерю данных, если анонсируемый маршрут не будет передавать трафик в анонсируемую сеть, направить трафик по неоптимальному пути и т. п.

3.2. Использование уязвимостей других протоколов

3.2.1. Сообщения TCP

BGP работает на основе протокола TCP, прослушивая порт 179. Следовательно, протокол BGP уязвим для атак на TCP.

3.2.1.1. TCP SYN

SYN flooding: Подобно другим протоколам, BGP зависит от воздействия на реализацию TCP атак с помощью лавины пакетов SYN, и должен использовать поддерживаемые реализацией механизмы защиты от этого типа атак.
Событие 14. Если внешний атакующий способен передавать SYN-пакеты узлу BGP с достаточной скоростью на этапе организации соединения, пакеты SYN от легитимного партнера будут представляться как другое соединение. Если атакующий способен продолжать передачу последовательности пакетов, приводящей к организации соединения BGP (например, угадывая порядковый номер узла BGP для пакетов SYN ACK), соединения от атакующего и легитимного узла могут вступить в конфликт. В зависимости от результатов детектирования конфликтов (если атакующий выбирает идентификатор BGP, как будто хочет выиграть скачки) корректное

соединение с легитимным партнером может быть разорвано. Использование [TCPMD5] может служить отражению таких атак.

3.2.1.2. TCP SYN ACK

Событие 16. Если внешний атакующий способен отвечать на SYN-пакеты узла BGP раньше легитимного партнера, в ответ на SYN-ACK от легитимного партнера будет передаваться пустой отклик ACK, заставляющий легитимного партнера передавать пакет RST, который будет разрывать соединение. Узел BGP будет разрывать соединение, освобождать связанные с ним ресурсы BGP, удалять все связанные с соединением маршруты и запускать процесс выбора маршрутов. Такая атака требует от внешнего атакующего предсказания порядковых номеров, используемых в пакетах SYN. Использование [TCPMD5] может служить отражению таких атак.

3.2.1.3. TCP ACK

Событие 17. Если внешний атакующий способен с достаточной скоростью передавать подставные пакеты ACK на этапе организации соединения, узел BGP может принять решение о завершении этапа организации соединения, передать пакет OPEN (Событие 17) и перейти в состояние OpenSent. Информация о доставке ACK от легитимного партнера не будет передаваться процессу BGP, поскольку будет воспринята как дубликат пакета. Таким образом, это сообщение не создает уязвимости BGP на этапе организации соединения. Подмена ACK после организации соединения требует точного предсказания используемого порядкового номера, что в общем случае является очень сложной задачей. Использование [TCPMD5] может служить отражению таких атак.

3.2.1.4. TCP RST/FIN/FIN-ACK

Событие 18. Если внешний атакующий способен генерировать подставные пакеты RST, узел BGP будет разрывать соединение, освобождать связанные с ним ресурсы BGP, удалять все связанные с соединением маршруты и запускать процесс выбора маршрутов. Если внешний атакующий способен генерировать подставные пакеты FIN, передача данных будет продолжаться, но любая попытка приема будет вызывать уведомление о закрытии соединения. В большинстве случаев это приведет к тому, что соединение будет переведено в состояние Idle. Однако соединения, находящиеся в момент атаки в состоянии Connect или OpenSent, будут возвращаться в состояние Active.
Генерация подставных пакетов RST в такой ситуации требует от атакующего предсказания порядкового номера, который должен попадать в окно приема [Watson04]. В общем случае это более простая задача, нежели точное предсказание порядкового номера, требуемое для успешной подмены FIN. Использование [TCPMD5] может служить отражению таких атак.

3.2.1.5. DoS и DDoS

Поскольку пакеты, направленные в порт TCP с номером 179, передаются процессу BGP, который потенциально является самым медленным процессом в маршрутизаторе, лавина пакетов, адресованных в порт TCP 179 маршрутизатора может использоваться как DoS-атака на маршрутизатор в целом. Протокол BGP не включает механизмов предотвращения таких атак и для их отражения нужны иные методы.

3.2.2. Прочие протоколы

3.2.2.1. Ручная остановка

Событие 2. Ручная остановка заставляет узел BGP разрывать соединение, освобождать связанные с ним ресурсы BGP, удалять все связанные с соединением маршруты и запускать процесс выбора маршрутов. Если механизм, используемый для уведомления узла BGP о ручной установке, недостаточно защищен, соединение BGP может быть разорвано внешним атакующим. Следовательно, безопасность BGP зависит от уровня безопасности протоколов управления и настройки, используемых для передачи сигнала о таких событиях.

3.2.2.2. Open Collision Dump

Событие 23. Событие OpenCollisionDump может генерироваться административным путем при обнаружении конфликта в соединении, если планируется разрыв этого соединения. Когда такое событие происходит, независимо от состояния соединения BGP, это соединение разрывается, освобождаются ресурсы BGP, удаляются связанные с соединением маршруты и т. д. Следовательно, безопасность BGP зависит от уровня безопасности протоколов управления и настройки, используемых для передачи сигнала о таких событиях.

3.2.2.3. Таймеры

События 9-13. Протокол BGP использует 5 таймеров (ConnectRetry, Hold, Keepalive, MinASOrigination-Interval, MinRouteAdvertisementInterval) и дополнительно может использовать еще 2 (DelayOpen и IdleHold). Эти таймеры играют важную роль в работе BGP. Например, при изменении значения таймера Hold удаленный партнер может решить, что соединение не отвечает и разорвать его, освободив ресурсы, удалив связанные маршруты и т. д. Следовательно, безопасность BGP зависит от уровня безопасности протоколов управления и настройки, используемых для управления таймерами.

4. Вопросы безопасности

Весь этот документ посвящен вопросам безопасности и включает анализ уязвимостей протокола BGP.
Использование обязательного для реализации механизма [TCPMD5] снижает уровень угрозы в результате вставки, изменения или удаления сообщений, а также атак с участием человека (man-in-the-middle) со стороны внешних узлов. Если желательно обеспечить конфиденциальность маршрутных данных (это спорный вопрос), эту задачу можно решить с помощью IPsec ESP.

4.1. Остаточный риск

Как криптографические механизмы, [TCPMD5] и IPsec [Ipsec] предполагают, что криптоалгоритм является безопасным, используемые секреты защищены от раскрытия и не могут быть угаданы, а также обеспечивается безопасное управление платформой, предотвращена возможность ее взлома и т. п.
Эти механизмы не предотвращают атак со стороны легитимных BGP-партнеров маршрутизатора. Существует несколько возможных решений для предотвращения вставки узлом BGP ложной информации в анонсы, рассылаемые партнерам (например, для организации атак на сети, из которых начинается маршрут, или AS-PATH):

1. Защита источника — подпись исходной AS.
2. Защита источника и соседей — подпись исходной AS или предшествующей информации ([Smith96])
3. Защита источника и маршрута — подпись исходной AS и подписи AS_PATH для маршрутизаторов, со стороны которых вы хотите предотвратить возможность атаки ([SBGP00]).
4. Фильтрация — основывается на проверке AS_PATH и NLRI исходной AS ([RPSL]).

Фильтрация используется в некоторых точках подключения пользователей, но неэффективна в «центральных узлах» Internet. Другие механизмы защиты пока обсуждаются и не нашли широкого применения.

4.2. Эксплуатационная защита

Протокол BGP используется прежде всего как средство предоставления данных о доступности автономных систем и распространения информации о доступности внешних сетей внутри AS. BGP является протоколом маршрутизации, используемым для распространения глобальной маршрутной информации в Internet. Следовательно, BGP используется всеми основными сервис-провайдерами (ISP), а также более мелкими провайдерами и другими организациями.
Роль BGP в Internet помещает реализации протокола BGP в уникальные условия и предъявляет к BGP уникальные требования в части безопасности. Протокол BGP используется на интерфейсах, связывающих провайдеров, где уровни трафика требуют использования специально разработанного оборудования для пересылки пакетов и на многие порядки превосходят возможности шифровального оборудования. Способность атакующего генерировать трафик для

организации DoS-атаки на рабочей станции с высокоскоростным интерфейсом значительно превосходит возможности программных систем шифрования или доступного по разумной цене криптографического оборудования, которые можно было бы использовать для детектирования такого трафика. В таких условиях основным средством защиты элементов сети от DoS-атак являются методы фильтрации пакетов на основе достаточно простых проверок. В результате для ISP, обслуживающих значительные объемы трафика, фильтрация пакетов по номерам портов является важным средством защиты от DoS-атак и необходимым дополнением к средствам криптографической инкапсуляции.
В современной практике ISP используют те или иные методы фильтрации общего назначения для снижения риска внешних атак. Для защиты внутренних сессий BGP (IBGP) фильтры реализуют на всех граничных узлах сети ISP. Эти фильтры блокируют весь трафик, адресованный внутренним элементам сети (обычно относящимся к одному префиксу) через порт BGP (179). При обнаружении номера порта BGP, пакеты из внутренней сети ISP не пересылаются с внутреннего интерфейса по адресу узла BGP, на котором поддерживаются внешние сессии BGP (EBGP), или адресам партнеров EBGP. Хорошо спроектированный и настроенный маршрутизатор способен ограничить риск компрометации, когда партнер BGP не может обеспечить должной фильтрации. Этот риск может быть ограничен также путем группировки сессий, в которых партнер не обеспечивает фильтрации, а также интерфейсов, через которые подключены партнеры.
Описанные выше меры существенно осложняют внешним узлам возможность организации DoS-атаки на ISP. Лишенный возможности создания требуемого для организации DoS-атаки внешнего трафика, злоумышленник вынужден будет использовать более сложные способы (например, взлом элементов сети ISP или перехват данных из физической среды).

5. Литература

5.1. Нормативные документы

1. [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997.
2. [TCPMD5] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.
3. [RFC4271] Rekhter, Y., Li, T., and S. Hares, Eds., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006

5.2. Дополнительная литература

4. [IPsec] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
5. [SBGP00] Kent, S., Lynn, C. and Seo, K., "Secure Border Gateway Protocol (Secure-BGP)", IEEE Journal on Selected Areas in Communications, Vol. 18, No. 4, April 2000, pp. 582-592.
6. [SecCons] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.
7. [Smith96] Smith, B. and Garcia-Luna-Aceves, J.J., "Securing the Border Gateway Routing Protocol", Proc. Global Internet '96, London, UK, 20-21 November 1996.
8. [RPSL] Villamizar, C., Alaettinoglu, C., Meyer, D., and S. Murphy, "Routing Policy System Security", RFC 2725, December 1999.
9. [Watson04] Watson, P., "Slipping In The Window: TCP Reset Attacks", CanSecWest 2004, April 2004.

Адрес автора

Sandra Murphy
Sparta, Inc.
7075 Samuel Morse Drive
Columbia, MD 21046
EMail: moc.sbalsit@ydnas

Перевод на русский язык

Николай Малых, ur.slocotorp@hkylamn

(source)