Содержание

Введение

Эта статья обсуждает, как Исследовательская группа уязвимости (VRT) определяет состояние правила в политике Проникновения по умолчанию, и как делает устройство Sourcefire, определяют соответствующее состояние по умолчанию для нового правила.

Определение управляет государством в политике по умолчанию

Каждое правило имеет поле метаданных с нулем или большими значениями политики. В настоящее время существует шесть возможных значений политики:

1. отбрасывание ips безопасности
2. предупреждение ips безопасности
3. отбрасывание сбалансированного ips
4. предупреждение сбалансированного ips
5. отбрасывание ips подключения
6. предупреждение ips подключения

Если политика IPS происходит от, скажем, предоставленной Sourcefire **Сбалансированной Безопасности и Политики подключений**, управляемое устройство находится во встроенном режиме, и правило имеет значение политики метаданных отбрасывания сбалансированного ips, правило будет установлено, чтобы отбросить и генерировать события в вашей политике IPS. Если правило будет иметь значение политики только отбрасывания ips безопасности, то оно будет отключено в вашей политике.

> **Примечание:** Если правилу задали значения несколька правил, например: отбрасывание ips безопасности политики, отбрасывание сбалансированного ips политики, это появляется в обеих политике. Если никакое значение политики не задано для данного правила, это не появляется ни в какой политике по умолчанию.

Если управляемое устройство установлено в пассивный режим, и политика собирается понизиться, это не имеет никакого эффекта. Устройство просто генерирует

предупреждения. Если устройство находится на встроенном режиме, и значение политики собирается понизиться, пакеты отбрасываний правила по умолчанию. Если его значение политики собирается предупредить, это только генерирует события без отбрасывания.

Наконец, в большинстве случаев, если пакет отброшен, предупреждение генерируется. Это истинно, пока подавление предупреждений независимо не настроено для данного правила.

Как делает Sourcefire, определяют соответствующее состояние по умолчанию, для нового правила

Состояние по умолчанию правила основывается на многих факторах. Пример:

Влияние

Что следует учесть

Как, вероятно, он, который попытки будут предприняты для использования этой уязвимости, и какой процент от наших пользователей (и клиенты Sourcefire и более широкое сообщество Фырканья), вероятно, будет уязвим для этой уязвимости?

Вещи помнить

Уязвимость Internet Explorer с известными методами атаки в дикой природе оказывает намного более высокое влияние, чем, скажем, функция базы данных SAP, которая может использоваться злонамеренно, когда разрешения неправильно настроены, или сложная атака отказ в обслуживании в неясном модуле Ядра Linux. VRT делает суждение влияния начиная со счета CVSS уязвимости, отрегулировав его по мере необходимости с любыми дополнительными сведениями, которыми мы можем обладать. Это - самая важная метрика всех, потому что мы будем иногда включать правило, иначе не включить / не, собираются понизиться, если влияние достаточно высоко.

Производительность

Что следует учесть

Мы ожидаем это правило быть быстрыми или медленными в "средней" сети?

Вещи помнить

В то время как скорость правила совершенно зависит от трафика, который она осматривает, который делает производительность трудной измериться, у нас есть общее представление того, что составляет стандартную сеть, и как данное правило выполняет на той стандартной сети. Мы также знаем, что правило с, например, одиночное соответствие содержания, которое относительно длинно (6 или больше байтов, как правило) и относительно уникально (т.е. "obscureJavaScriptFunction ()", и не "|00 00 00 00 |" или "GET / HTTP/1.1") оценит быстрее, чем правило со сложным PCRE, серией byte_test и/или byte_jump пунктов, и т.д. С этим знанием мы можем определить, будет ли правило быстро или замедлит и примет это во внимание.

Уверенность

Что следует учесть

Как, вероятно, это правило состоит в том, чтобы генерировать ошибочные допуски?

Вещи помнить

Некоторые уязвимости требуют очень определенный, легко обнаруженные условия присутствовать, чтобы быть использованными, в этом случае мы можем быть очень уверены, что любое время связанные огни правила, оперативное использование происходит. Например, если существует переполнение буфера в протоколе, который имеет уникальную волшебную строку в фиксированной позиции, и затем указанную длину, которая является неподвижным расстоянием далеко от той волшебной строки, мы можем быть уверены в нашей способности найти волшебную строку и проверить его против известного значения для проблем. В других случаях проблемы намного менее четко определены; например, определенные атаки отравления кэшем DNS могут быть обозначены неправильно большим числом ответов NXDOMAIN, прибывающих из сервера в определенный период времени. В таком случае простое присутствие ответа NXDOMAIN не находится в и себя индикатор использования; это - присутствие очень большого числа таких ответов в скором времени, которое указывает на проблему. Так как тот номер будет другим для других сетей, VRT вынужден выбрать значение, которое должно работать для большинства сетей и выпуска это; однако, мы не можем быть на 100% уверены, что, когда правило срабатывает, происходят фактические нежелательные действия.

Наконец, но не в последнюю очередь, в то время как другие факторы можно время от времени рассматривать как релевантные, влияние является королем в конце дня - проверка, что наши клиенты защищены против угроз, которые они, скорее всего, будут видеть в дикой природе, наше основное предприятие.