Содержание

Введение

Исследовательская группа уязвимости (VRT) освобождает Обновление правила Sourcefire (SRU) для адресации к последним угрозам и уязвимостям. Новый выпуск SRU может содержать обновленную основную политику для использования в установке Фырканья. Этот документ объясняет процесс, используемый Исследовательской группой Уязвимости для решения, как правила назначены на каждую политику.

Метрики, используемые для определения Ruleset По умолчанию

- Основная используемая метрика является счетом Общей системы выигрыша уязвимости (CVSS), назначенным на каждую уязвимость, которая могла бы быть охвачена правилом.
- Вторая метрика временная основанный и касается возраста определенной уязвимости.
- Заключительная метрика является определенной областью покрытия для правила. Так, например, правила Инжекции SQL, как полагают, достаточно важны для имения влияния, будучи рассмотренным для включения политики.

  Примечание: Уязвимости, охваченные правилами в этих категориях, считают важными, независимо от возраста.

Подключение по политике ядра безопасности

1. Счет CVSS должен быть 10

2. Возраст уязвимости

   - Текущий год (2014, например)
   - В прошлом году (2013 в данном примере)
   - Год прежде в последний раз (2012 в данном примере)

3. Категория правила

   - Не используемый для этой политики

Сбалансированная основная политика

> **Примечание: Сбалансированная** политика является состоянием поставки по умолчанию VRT Ruleset для Фырканья С открытым исходным кодом.

1. Счет CVSS 9 или больше

2. Возраст уязвимости

   - Текущий год (2014, например)
   - В прошлом году (2013 в данном примере)
   - Год прежде в последний раз (2012 в данном примере)

3. Категория правила

   - Вредоносный CNC
   - Черный список
   - Инжекция SQL
   - Набор использования

Безопасность по политике ядра подключения

1. Счет CVSS 8 или больше

2. Возраст уязвимости

   - Текущий год (2014, например)
   - В прошлом году (2013 в данном примере)
   - Год прежде в последний раз (2012 в данном примере)
   - Предшествующий год (2011 в данном примере)

3. Категория правила

   - Вредоносный CNC
   - Черный список
   - Инжекция SQL
   - Набор использования
   - Приложение - обнаруживает

Частота обновлений политики

Все новые правила размещены в один или больше основной политики на основе определенных критериев. Политика переоценивается каждый год, и правила с предыдущих лет, как возраст уязвимостей, удалены из политики для поддержания политики в соответствии с условиями выбора.

Если перемещение правил между категориями, их присутствие в политике также решено на основе процесса выбранной категории. Аналогично, должен изменение счета CVSS к определенной уязвимости, которая охвачена правилом, это - присутствие в политике на

основе метрики CVSS, также переоценен.

Примечание: Правила в перечисленной политике оценены на правиле основанием правила. Будут некоторые правила, которые являются более старыми, а не в критериях выше этого будет в политике по умолчанию. Вышеупомянутое является условиями выбора для стандартных правил и всегда подвержено изменениям основанное на среде угрозы.