Устранение проблем переопределений действия при событии

Введение

Этот документ описывает возможные проблемы, вызванные переопределениями действия при событии на системе предотвращения вторжений Cisco (IPS) (IPS), и предлагает рекомендации настроить и устранить неполадки вашей установки.

> **Примечание:** Переопределения действия при событии являются глобальными действиями, взятыми подписи, основанные на оценке риска. Как с любой глобальной конфигурацией, примите большие меры с изменениями конфигурации и добавлениями.

Проблемы переопределения действия при событии

Описание

Когда то событие находится в пределах указанного диапазона оценки риска, переопределения действия при событии добавляют дополнительные действия к событию подписи. Используйте переопределения действия при событии тщательно. Iif вы создаете замену с широким диапазоном оценки риска для события, которое часто инициируется (особенно определенные, дорогие действия, такие как действия регистрации IP), вы могли бы вызвать проблемы.

Влияние

Чрезмерные записи к хранилищу события, как правило, привязываются к высокой загрузке ЦП и общей безразличности датчика к программным средствам управляющего доступ, таким как интерфейс командной строки (CLI) и Cisco IPS Device Manager (IDM).

Действия Регистрации IP и дескрипторы файла

Дескриптор файла является структурой данных, используемой программой для получения маркера на файле; известные дескрипторы 0,1,2 для стандарта в, стандарт и стандартная ошибка. Когда процесс открывает новый файл или сокет, дескриптор файла создан.

При создании переопределения действия при событии для действия регистрации IP, такого как регистрационные пакеты атакующего, регистрационные парные пакеты или регистрационные пакеты жертвы, это могло бы исчерпать пул дескрипторов файла; на полную производительность датчика можно было бы негативно влиять, и датчик может не

функционировать должным образом.

Действия TRAP-СООБЩЕНИЯ SNMP и переопределения действия при событии

Подпись, которая имеет только одиночное действие trap-сообщения snmp запроса также, генерирует аварийное событие, которое записано в хранилище события. Так, чрезмерное увольнение действия Перехвата простого протокола управления сетью (SNMP) могло бы также инициировать те же проблемы, замеченные с чрезмерными действиями предупреждения продукта.

Действия для подписей механизма нормализатора

Не добавляйте действие, которое вызывает записи хранилища события (те, которые производят предупреждение, trap-сообщение snmp запроса или регистрационные действия) к подписям Нормализатора. Это применяется ко всем 1200-1330 идентификаторам подписи диапазона.

За исключением кратких сценариев устранения проблем, вы не должны использовать переопределения действия при событии для подписей механизма Нормализатора. Это может быть особенно проблематично в:

- высоко фрагментированные сценарии IP (из-за подписей с 1200 диапазонами)
- в большой степени неисправные (ооо) сценарии TCP (подписи с 1300 диапазонами)

Например, переопределение действия при событии, которое вызывает запись к хранилищу события для каждого ооо пакета TCP, может вызвать проблемы использования и ресурс.

Переопределения действия при событии с оценкой риска 0-100

В целом избегите переопределений действия при событии с оценкой риска 0-100, потому что низкая оценка может поместить ваш датчик из-за опасности сбоя при определенных обстоятельствах.

Подписи компонента Меты часто запускают за на вид мягкий (и распространенный) типы трафика. Подписи Меты ищут комбинацию одной или более подписей компонента Меты для инициирования, прежде чем подпись родителя Меты запустит предупреждение. Подписи компонента Меты, по умолчанию, не имеют никаких действий, привязанных к ним; это является намеренным, потому что они часто совпадают на общем трафике. Подписи компонента Меты имеют основную оценку риска по умолчанию 15. Для исключения перехвата этих соответствий подписи в переопределении действия при событии Cisco рекомендует не использовать риск, оценивающий ниже, чем 25 при создании переопределения действия при событии; т.е. оценка риска не должна быть ниже 25-100.

Проверьте использование IPS

Команды

Примечание: Чтобы получить подробные сведения о командах в данном документе,

[используйте Средство поиска команд (только для зарегистрированных клиентов)]

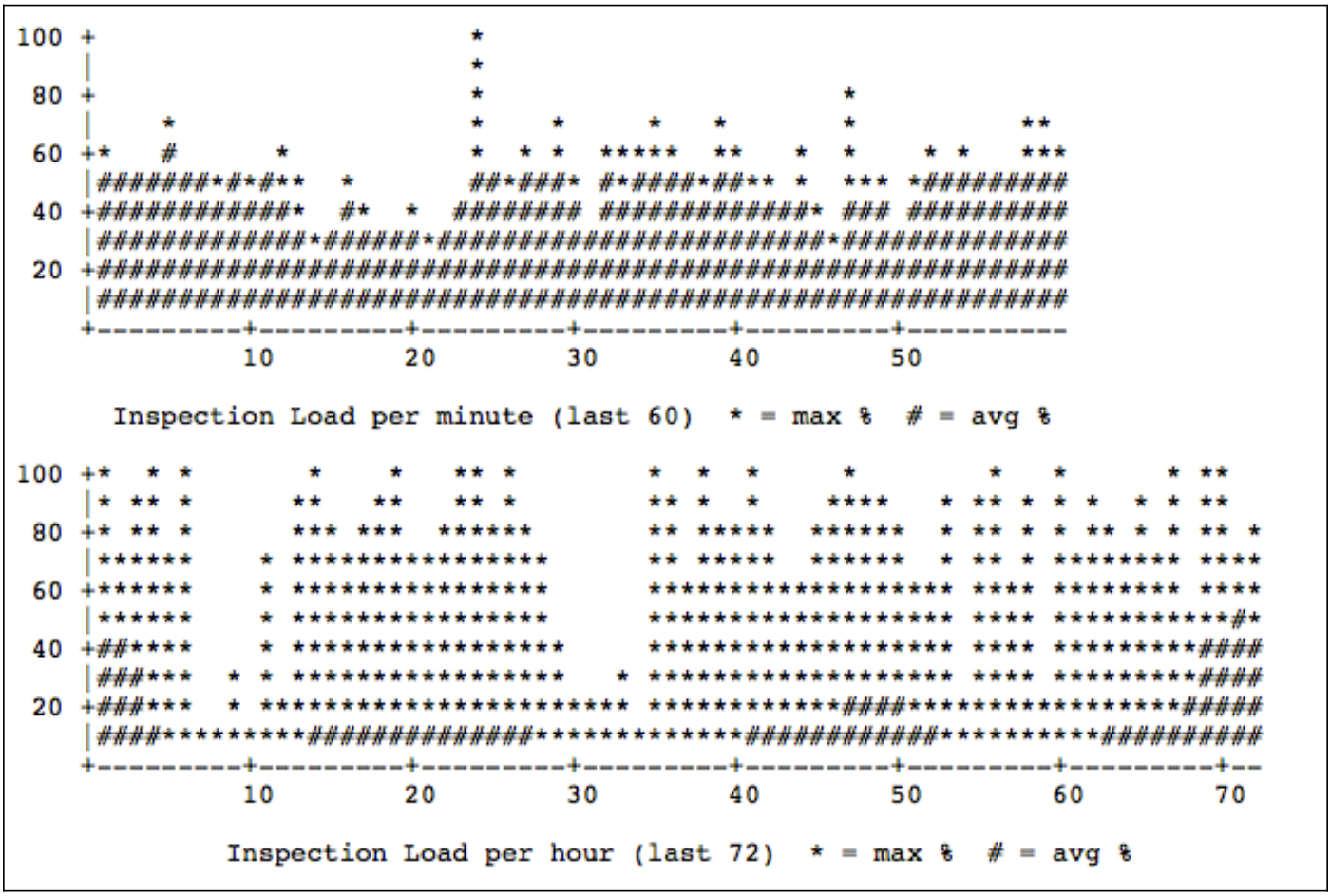
Введите команду **действительного датчика статистики показа** в CLI для поиска инспекционного процента загрузки:

```
sensor# show statistics virtual-sensor | inc Load
Processing Load Percentage = 100
```

В Версиях IPS 7.0 (8) E4 и 7.1 (6) E4, была добавлена **команда inspection-load показа**:

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```

Это - пример выходных данных от той команды:



Очень процент высокой нагрузки (90% или выше) мог бы указать, что существуют чрезмерные события, инициированные переопределениями действия при событии. См. журналы для дальнейшего подтверждения этой возможности.

Журналы

Основной индикатор чрезмерных переопределений действия при событии является быстрой накруткой хранилища события, как замечено в данном примере main.log файл:

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```

В целом хранилище события, переносящееся, который происходит чаще, чем раз в час, может указать на проблему. В некоторых сценариях накрутка является столь чрезмерной, что она может происходить много раз в течение минуты. Существует много переменных, таких как возможность общей производительности платформы, для рассмотрения.

Устранение неполадок

Определите, какое событие, трафик или действие вызывают проблему переопределения действия при событии. Это - предупреждение продукта, регистрация IP, подпись Нормализатора или подпись компонента Меты?

- Если это - 'болтливая' подпись, и вы решаете, что подпись создает ошибочные допуски для событий, запишите фильтр действия события (EAF).
- Для регистрации IP Cisco рекомендует, чтобы вы избежали EAFs или использовали EAFs с осторожностью и с полным пониманием рисков.
- Подписи нормализатора и подписи компонента Меты не должны иметь аварийного действия за исключением временных сценариев устранения проблем.

Дополнительные сведения

- Переопределения действия при событии Настройки
- Руководства по конфигурации IPS
- Cisco Systems – техническая поддержка и документация