Contenido

Introducción

El equipo de investigación de la vulnerabilidad (VRT) libera la actualización de la regla de Sourcefire (SRU) para dirigir las últimas amenazas y vulnerabilidades. Una nueva versión SRU puede contener la directiva baja actualizada para el uso en una instalación del Snort. Este documento explica el proceso usado por el equipo de investigación de la vulnerabilidad para decidir a cómo las reglas se asignan a cada directiva.

Métrica usada para determinar Ruleset predeterminado

- El métrico principal usado es la calificación común del sistema de calificación de la vulnerabilidad (CVSS) asignada a cada vulnerabilidad que se pudo cubrir por una regla.
- El segundo métrico es haber basado temporal y se refiere a la edad de una vulnerabilidad determinada.
- El métrico final es la área determinada de cobertura para la regla. Tan por ejemplo, las reglas de la inyección SQL se consideran ser bastante importantes tener influencia al ser considerado para la inclusión de la directiva.

  Nota: Las vulnerabilidades cubiertas por las reglas en estas categorías se consideran importantes, sin importar la edad.

Conectividad sobre la directiva de la base de Seguridad

1. La calificación CVSS debe ser 10

2. Edad de la vulnerabilidad

   - Año en curso (2014 por ejemplo)
   - El año pasado (2013 en este ejemplo)
   - Año antes del último (2012 en este ejemplo)
3. Categoría de la regla

   - No utilizado para esta directiva

Directiva baja equilibrada

> Nota: La directiva **equilibrada** es el estado del envío por defecto del VRT Ruleset para el Snort del código abierto.

1. Calificación 9 CVSS o mayor

2. Edad de la vulnerabilidad

   - Año en curso (2014 por ejemplo)
   - El año pasado (2013 en este ejemplo)
   - Año antes del último (2012 en este ejemplo)
3. Categoría de la regla

   - Malware-CNC
   - Lista negra
   - Inyección SQL
   - Exploit-equipo

Seguridad sobre la directiva de la base de la Conectividad

1. Calificación 8 CVSS o mayor

2. Edad de la vulnerabilidad

   - Año en curso (2014 por ejemplo)
   - El año pasado (2013 en este ejemplo)
   - Año antes del último (2012 en este ejemplo)
   - Año anteriormente (2011 en este ejemplo)
3. Categoría de la regla

   - Malware-CNC
   - Lista negra
   - Inyección SQL
   - Exploit-equipo
   - APP-detecte

Frecuencia de las actualizaciones de la directiva

Todas las nuevas reglas se ponen en uno o más de las directivas bajas basadas en los criterios identificados. Las directivas se valoran de nuevo cada año, y las reglas a partir de los años pasados, mientras que las vulnerabilidades envejecen, se quitan de una directiva para mantener la directiva obediente con el Criterio de selección.

Si las reglas se mueven entre las categorías, su presencia en las directivas también se decide sobre la base del proceso de la selección de categoría. Asimismo, el cambio de la calificación CVSS para una vulnerabilidad determinada que sea cubierta por una regla, es presencia en una

directiva basada en el CVSS métrico también se valora de nuevo.

> Nota: Las reglas en las directivas mencionadas son evaluadas en una regla por la base de la regla. Habrá algunas reglas que son más viejas y no en los criterios sobre eso esté en las políticas predeterminadas. El antedicho es el Criterio de selección para las reglas predeterminadas, y está siempre conforme al cambio basado sobre el paisaje de la amenaza.