Contenido

Introducción

Este artículo discute cómo el equipo de investigación de la vulnerabilidad (VRT) determina el estado de la regla en las directivas predeterminadas de la intrusión, y cómo hace una aplicación de Sourcefire determine el estado predeterminado apropiado para una nueva regla.

Determinación del estado de la regla en una política predeterminada

Cada regla tiene un campo de los meta datos, con cero o más valor de directiva. Hay actualmente seis valores de directiva posibles:

1. Seguridad-IPS de descenso
2. alerta Seguridad-IPS
3. equilibrado-IPS de descenso
4. alerta equilibrado-IPS
5. Conectividad-IPS de descenso
6. alerta Conectividad-IPS

Si una directiva IPS se desciende, por ejemplo, del Sourcefire-proporcionó a la **Seguridad y a la política de conectividad equilibradas**, el dispositivo administrado está en el modo en línea, y una regla tiene un valor de directiva de los meta datos del descenso equilibrado-IPS, la regla será fijada para caer y para generar los eventos en su directiva IPS. Si una regla tiene un valor de directiva solamente del descenso Seguridad-IPS, será inhabilitada en su directiva.

> Nota: Si una regla tiene valores de políticas múltiples especificados, por ejemplo: descenso Seguridad-IPS de la directiva, descenso equilibrado-IPS de la directiva, aparece en ambas directivas. Si no se especifica ningún valor de directiva para una regla dada, aparece en ningunas directivas por abandono.

Si un dispositivo administrado se fija al modo pasivo, y una directiva se fija para caer, ésta no tiene ningún efecto. El dispositivo genera simplemente las alertas. Si un dispositivo está en el modo en línea, y un valor de directiva se fija para caer, la regla cae los paquetes por abandono. Si su valor de directiva se fija para alertar, genera solamente los eventos, sin la caída.

Finalmente, en la mayoría de los casos, si se cae un paquete, se genera una alerta. Esto es verdad a menos que la supresión de las alertas se configure independientemente para una regla dada.

Cómo hace Sourcefire determine un estado predeterminado apropiado, para una nueva regla

El estado predeterminado de una regla se basa en varios factores. Por ejemplo:

Impacto

Puntos a considerar

¿Cómo está probablemente que las tentativas serán hechas para explotar esta vulnerabilidad, y qué porcentaje de nuestros usuarios (los clientes de Sourcefire y la comunidad más amplia del Snort) es probable ser vulnerable a esta vulnerabilidad?

Cosas a recordar

Una vulnerabilidad del Internet Explorer con los ataques conocidos en el salvaje tiene mucho más de alto impacto que, por ejemplo, una función de la base de datos de SAP que se pueda utilizar malévolo cuando los permisos se configuran incorrectamente, o un establecimiento de rechazo del servicio complejo en un módulo indeterminado del núcleo de Linux. VRT hace un juicio del impacto que comienza con la calificación CVSS de una vulnerabilidad, ajustándolo cuanto sea necesario con cualquier información adicional que poder poseer. Éste es el métrico más importante de todos, porque habilitaremos a veces una regla no conseguiríamos de otra manera encendido dado vuelta/para no conseguir el conjunto para caer si es el impacto arriba bastante.

Rendimiento

Puntos a considerar

¿Esperamos que esta regla sea rápida o lenta en una red “media”?

Cosas a recordar

Mientras que la velocidad de una regla es totalmente dependiente en el tráfico que está examinando, que hace el funcionamiento difícil medir, tenemos una idea general de qué constituye una red normal, y de cómo una regla dada se realiza en esa red normal. También sabemos que una regla con, por ejemplo, una sola coincidencia contenta que sea relativamente larga (6 o más bytes, típicamente) y relativamente único (es decir “obscureJavaScriptFunction()”, y no "|00 00 00 00|" o “GET/el HTTP/1.1") evaluará más rápidamente que una regla con un PCRE complejo, una serie de las cláusulas más byte_test y/o del byte_jump, etc. Con este conocimiento podemos determinar si una regla es rápida o lenta y toma eso en la consideración.

Confianza

Puntos a considerar

¿Cómo está probablemente esta regla para generar los falsos positivos?

Cosas a recordar

Algunas vulnerabilidades requieren las condiciones muy específicas, fácilmente detectadas para estar presentes para ser explotado, en este caso podemos sentirnos muy confiados que la regla asociada enciende en cualquier momento, un exploit vivo están en curso. Por ejemplo, si hay un desbordamiento de búfer en un protocolo que tenga una cadena mágica única en un de posición fija, y entonces una longitud especificada que sea una distancia fija lejos de esa cadena mágica, podemos sentirnos confiados en nuestra capacidad de encontrar la cadena mágica y de marcarla contra un valor conocido para los problemas. En otros casos, los problemas están mucho menos bien definidos; por ejemplo, ciertos ataques del envenenamiento del caché DNS se pueden indicar por anormalmente un número grande de contestaciones NXDOMAIN que vienen de un servidor en cierto período de tiempo. En tal caso, la simple presencia de una contestación NXDOMAIN no es de por sí un indicador de un exploit; es la presencia de un gran número de tales contestaciones en poco tiempo que indica el problema. Puesto que ese número será diferente para diversas redes, el VRT se fuerza para elegir un valor que deba trabajar para la mayoría de las redes y liberar eso; sin embargo, no podemos ser el 100% confiado eso, cuando están ocurriendo los fuegos de la regla, actividad maliciosa real.

En por último, mientras que otros factores se pueden considerar de vez en cuando como relevantes, el impacto es rey al final del día - aseegurandose a nuestros clientes se protegen contra las amenazas que son más probable de ver que en circulación es nuestro problema principal.