Contenido

Introducción

Este documento describe los cambios del comportamiento introducidos por las nuevas firmas después de poner al día el (IPS) del Cisco Intrusion Prevention System a un nuevo paquete de la firma.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Característica de la actualización de firma en el IPS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Series Sensores IPS 4XXX
- Serie ASA 5585-X IPS SSP
- Serie ASA 5500-X IPS SSP
- Serie ASA 5500 IPS SS

Versión 7.1(10)E4

Versión 7.3(4)E4

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Problema

Podría haber problemas múltiples tales como caídas de paquetes y los problemas de conectividad con ciertas aplicaciones después de realizar una actualización de firma en el IPS.To resuelven problemas tales problemas que sería muy útil si usted puede entender que los cambios en el

conjunto de firmas activo fijan la actualización de firma.

Solución

Paso 1.

La primera cosa que usted necesita marcar es el historial de la actualización para la firma. Esto dice el paquete anterior de la firma que se ejecutaba en el IPS y la versión actual del paquete de la firma.

Esto se puede descubrir de la salida del comando show version o del historial de la actualización la sección del snippet **tecnología de la demostración** lo mismo se menciona aquí:

Historial de la actualización

*** IPS-sig-S733-req-E4 19:59:50 UTC Fri 9 de agosto de 2015**

IPS-sig-S734-req-E4.pkg 19:59:49 UTC Tue 13 de agosto de 2015

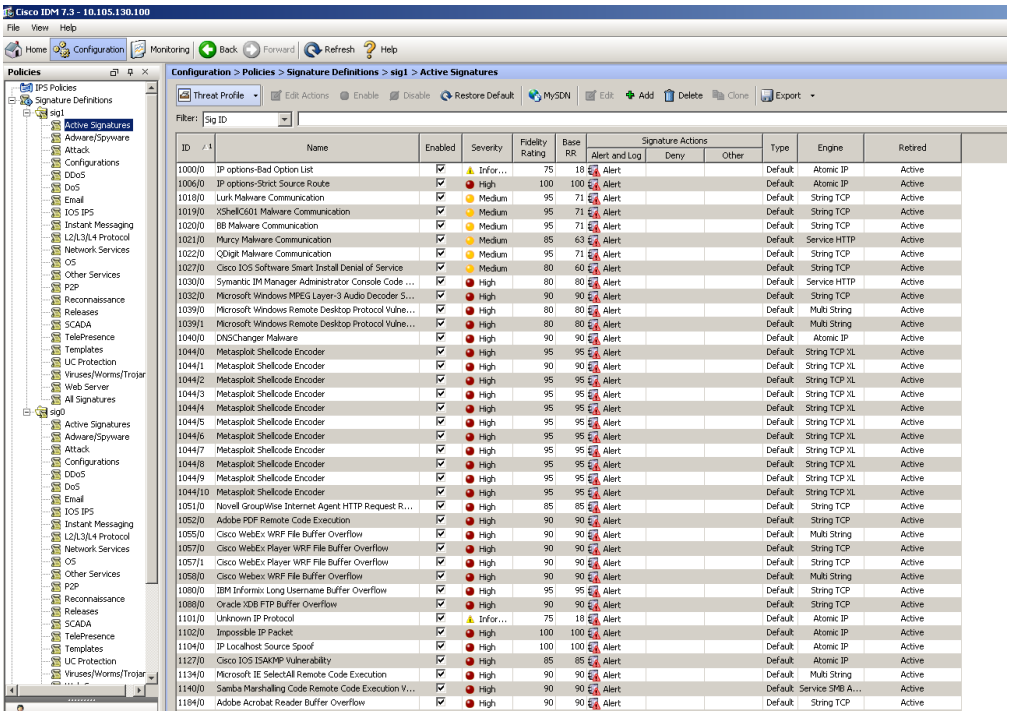
Ahora usted puede hacer que el paquete anterior de la firma que se ejecutaba en el IPS era s733 y se ha actualizado a s734 que es paquete actual de la firma.

Paso 2.

El segundo paso es entender los cambios se han realizado que y que se pueden marcar con el IME/IDM.

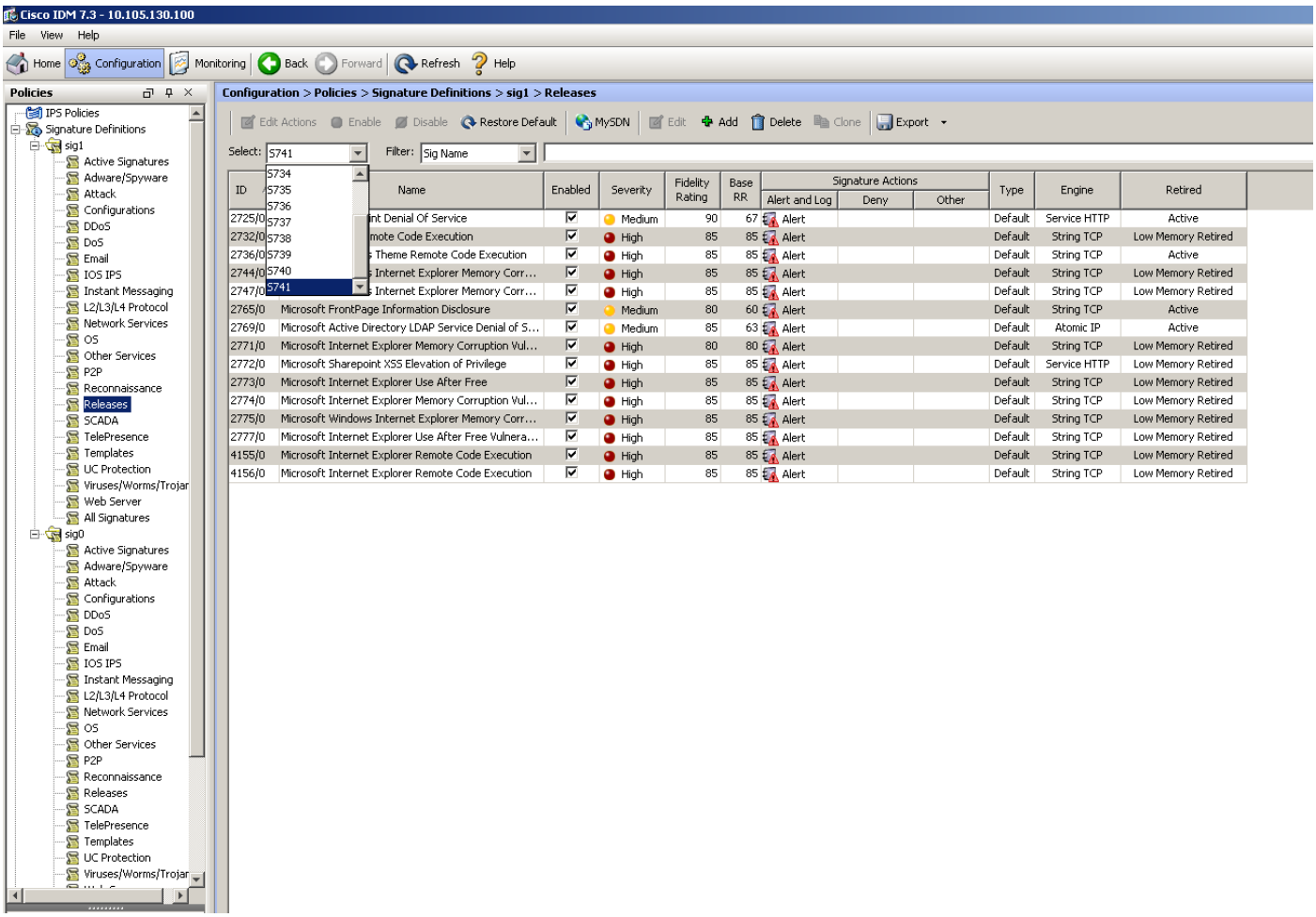
1. La lengueta activa de la firma en el IME/IDM se muestra en esta imagen.

Navegue a la **configuración > a las directivas > a las definiciones de la firma > a Sig1 > las firmas activas.**



2. Esta imagen muestra cómo seleccionar una versión específica de la firma.

Navegue a la **configuración > a las directivas > a las definiciones de la firma > a Sig1 > a las versiones.**



Fomente usando la opción de filtro que usted ha obtenido todas las firmas de una versión determinada, usted puede filtrarlas basó en el motor, la fidelidad, la gravedad etc.

De esta manera usted debe poder estrecharse abajo en los cambios en la versión de la firma que puede ser una causa potencial para el problema basado en cuál usted alinea su troubleshooting.