

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

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.

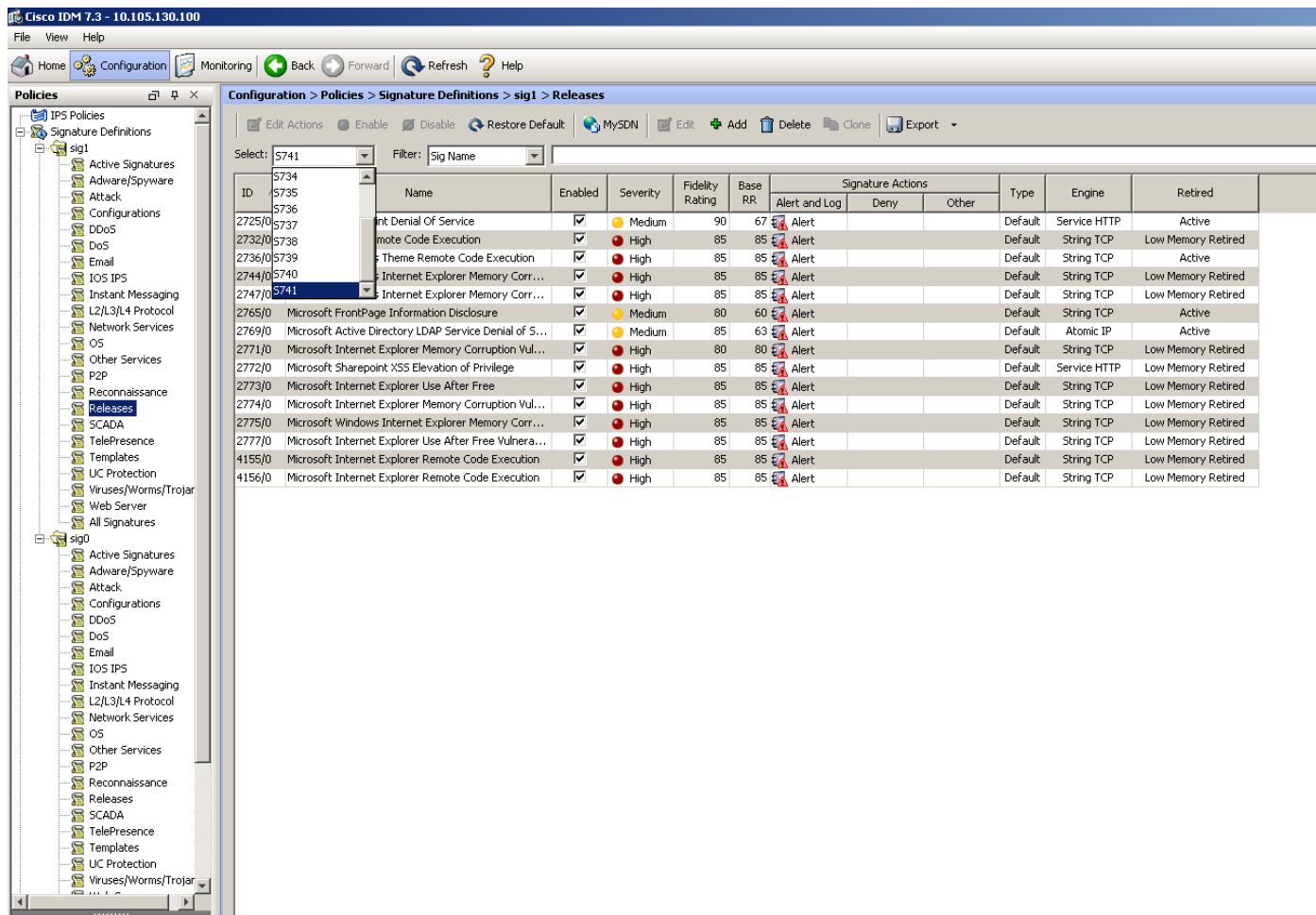
1. La lengüeta activa de la firma en el IME/IDM se muestra en esta imagen.

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

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions	Type	Engine	Retired
1000/0	IP options-Bad Option List	<input checked="" type="checkbox"/>	Info	75	18	Alert	Default	Atomic IP	Active
1006/0	IP options-Strict Source Route	<input checked="" type="checkbox"/>	High	100	100	Alert	Default	Atomic IP	Active
1010/0	Lark Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	Alert	Default	String TCP	Active
1019/0	XShellCGI Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	Alert	Default	String TCP	Active
1020/0	BB Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	Alert	Default	String TCP	Active
1021/0	Murcy Malware Communication	<input checked="" type="checkbox"/>	Medium	85	63	Alert	Default	Service HTTP	Active
1022/0	QDigt Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	Alert	Default	String TCP	Active
1027/0	Cisco IOS Software Smart Install Denial of Service	<input checked="" type="checkbox"/>	Medium	80	60	Alert	Default	String TCP	Active
1030/0	Symantec IM Manager Administrator Console Code ...	<input checked="" type="checkbox"/>	High	80	80	Alert	Default	Service HTTP	Active
1032/0	Microsoft Windows MPEG Layer3 Audio Decoder S...	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	String TCP	Active
1039/0	Microsoft Windows Remote Desktop Protocol Vuln...	<input checked="" type="checkbox"/>	High	80	80	Alert	Default	Multi String	Active
1039/1	Microsoft Windows Remote Desktop Protocol Vuln...	<input checked="" type="checkbox"/>	High	80	80	Alert	Default	Multi String	Active
1040/0	DNSChanger Malware	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	Atomic IP	Active
1044/0	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1044/1	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	String TCP XL	Active
1044/2	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1044/3	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1044/4	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1044/5	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1044/6	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1044/7	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1044/8	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1044/9	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1044/10	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP XL	Active
1051/0	Novell GroupWise Internet Agent HTTP Request R...	<input checked="" type="checkbox"/>	High	85	85	Alert	Default	String TCP	Active
1052/0	Adobe PDF Remote Code Execution	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	String TCP	Active
1055/0	Cisco WebEx WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	Multi String	Active
1057/0	Cisco WebEx Player WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	String TCP	Active
1057/1	Cisco WebEx Player WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	String TCP	Active
1058/0	Cisco WebEx WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	Multi String	Active
1080/0	IBM Informix Long Username Buffer Overflow	<input checked="" type="checkbox"/>	High	95	95	Alert	Default	String TCP	Active
1088/0	Oracle XDB FTP Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	String TCP	Active
1101/0	Unknown IP Protocol	<input checked="" type="checkbox"/>	Info	75	18	Alert	Default	Atomic IP	Active
1102/0	Impossible IP Packet	<input checked="" type="checkbox"/>	High	100	100	Alert	Default	Atomic IP	Active
1109/0	IP Localhost Source Spoof	<input checked="" type="checkbox"/>	High	100	100	Alert	Default	Atomic IP	Active
1127/0	Cisco IOS ISANMP Vulnerability	<input checked="" type="checkbox"/>	High	85	85	Alert	Default	Atomic IP	Active
1134/0	Microsoft IE Selected Remote Code Execution	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	Multi String	Active
1140/0	Samba Marshalling Code Remote Code Execution V...	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	Service SMB A...	Active
1184/0	Adobe Acrobat Reader Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert	Default	String TCP	Active

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.