

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Problème](#)

[Solution](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit les modifications comportementales introduites par les nouvelles signatures après mise à jour du Système de protection contre les intrusions Cisco (IPS) à un nouveau module de signature.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Caractéristique de mise à jour de signature sur l'IPS

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Capteurs de gamme IPS 4XXX
- Gamme ASA 5585-X IPS SSP
- Gamme ASA 5500-X IPS SSP
- Gamme de SSM ASA 5500 IPS

Version 7.1(10)E4

Version 7.3(4)E4

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Problème

Il pourrait y avoir de plusieurs questions telles que des pertes de paquets et les problèmes de connectivité avec certaines applications après avoir exécuté une mise à jour de signature sur l'IPS. To dépannent de telles questions qu'il serait très utile si vous pouvez comprendre que les

changements de la signature active réglée signalent la mise à jour de signature.

Solution

Étape 1.

La première chose que vous devez vérifier est l'historique de mise à jour pour la signature. Ceci indique le paquet précédent de signature qui s'exécutait sur l'IPS et la version en cours du paquet de signature.

Ceci peut être découvert de la sortie du **show version de** commande ou de l'historique de mise à jour la section de l'extrait **technologie d'exposition de la** même chose est mentionnée ici :

Historique de mise à jour

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

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

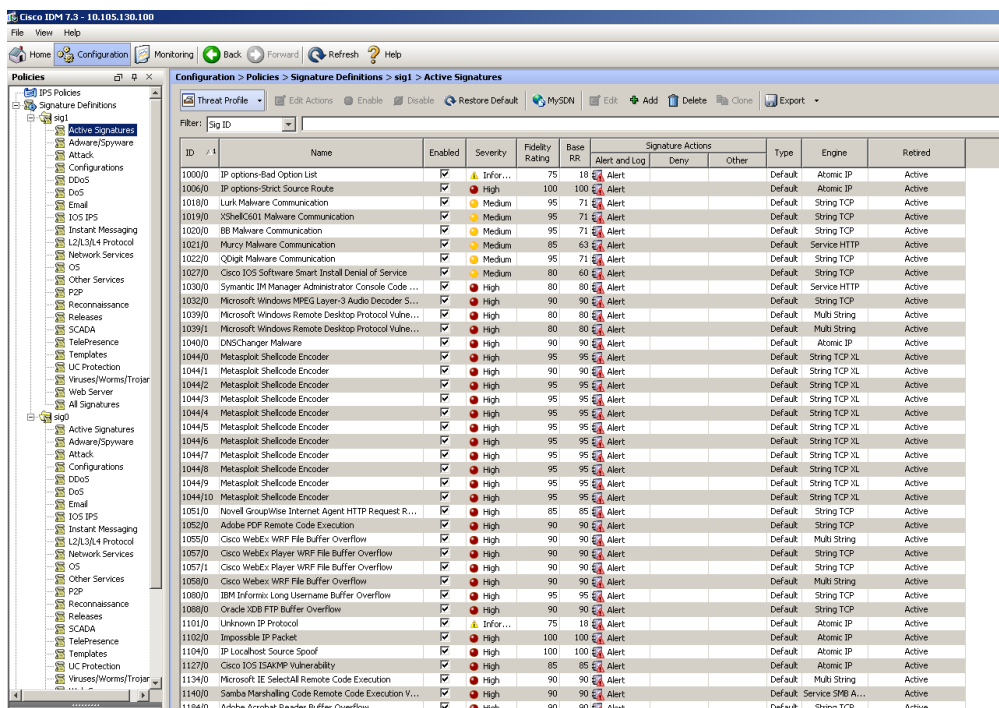
Maintenant vous pouvez faire que le paquet précédent de signature qui s'exécutait sur l'IPS était s733 et a été mis à jour à s734 qui est paquet en cours de signature.

Étape 2.

La deuxième étape est de comprendre les modifications qui ont été apportées et qui peuvent être vérifiées par l'IME/IDM.

1. L'onglet actif de signature sur l'IME/IDM est affiché dans cette image.

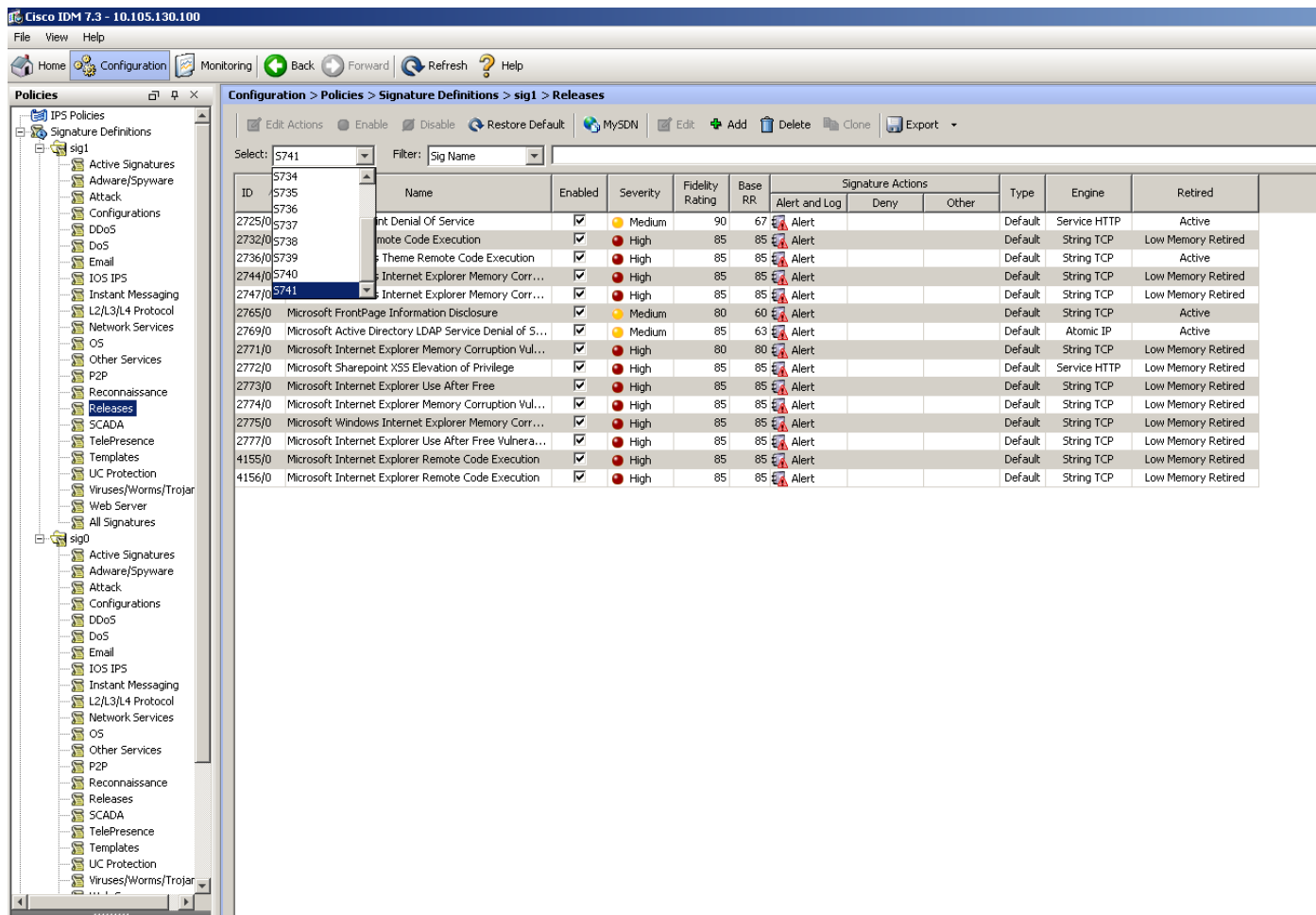
Naviguez vers la **configuration > les stratégies > les définitions de signature > le Sig1 > les signatures actives.**



ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions	Type	Engine	Retired
1000/0	IP options-Bad Option List	<input checked="" type="checkbox"/>	High	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	QOight 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	Symantic 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 Vuine...	<input checked="" type="checkbox"/>	High	80	80	Alert	Default	Multi String	Active
1039/1	Microsoft Windows Remote Desktop Protocol Vuine...	<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"/>	High	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 ISAMP 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. Cette image affiche comment sélectionner une release spécifique de signature.

Naviguez vers la configuration > les stratégies > les définitions de signature > le Sig1 > les releases.



Promouvez utilisant l'option de filtre que vous avez obtenu toutes les signatures d'une release particulière, vous peut les filtrer a basé sur l'engine, la fidélité, la sévérité etc.

Ce faisant, vous devez pouvoir se rétrécir vers le bas sur les changements de la release de signature qui peut être une cause potentielle pour la question basée sur ce que vous alignez votre dépannage.