Contenu

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

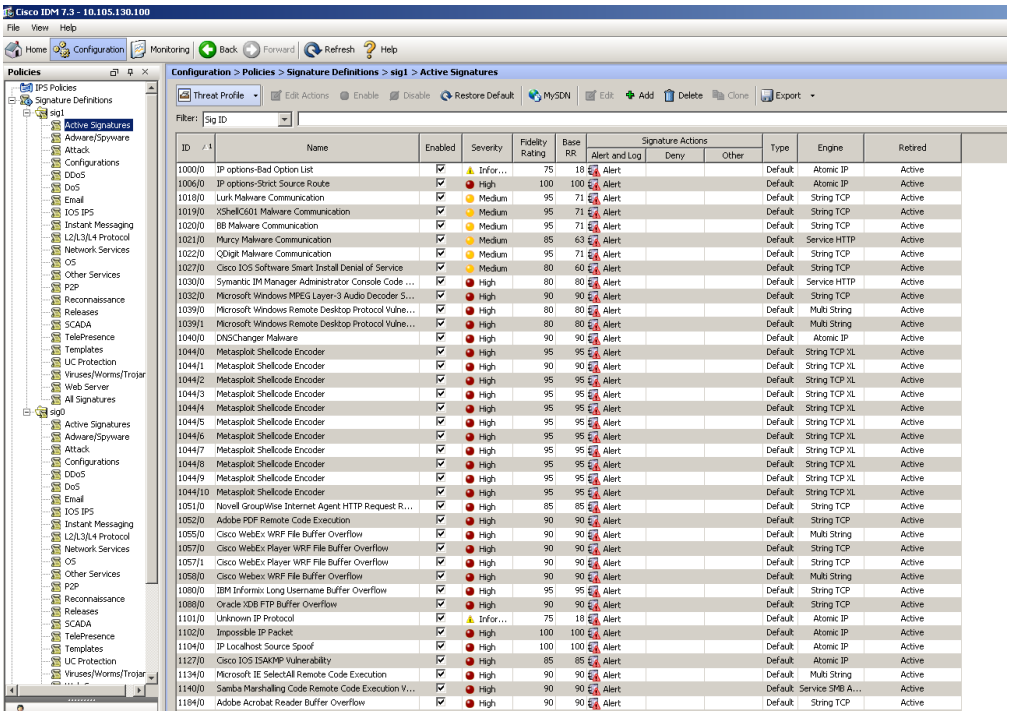
Maintenant vous pouvez faire que le paquet précédent de signature qui s'exécutait sur l'IPS était s733 et a été mis à jour à s734 qui est paquet en cours de signature.

Étape 2.

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

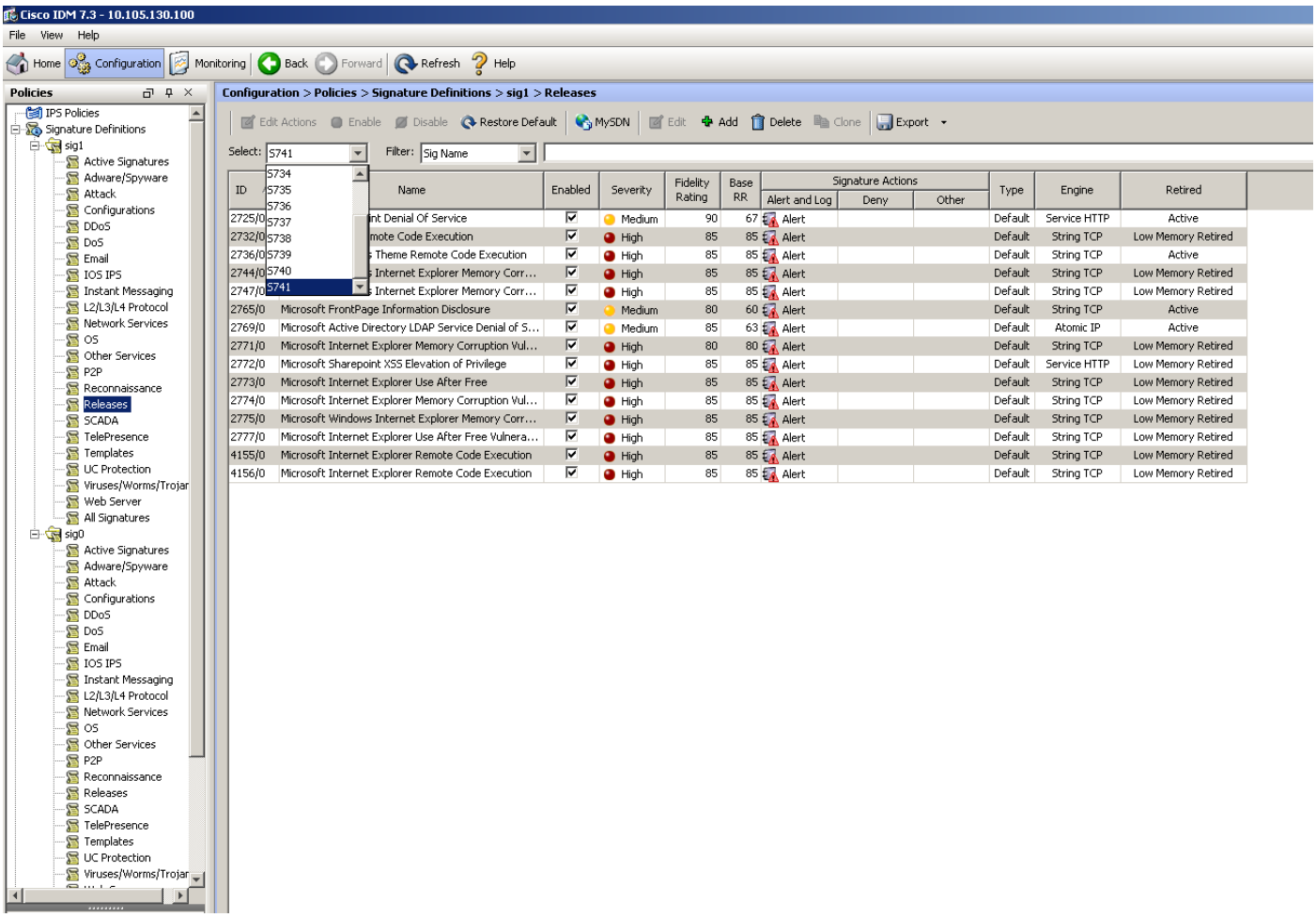
1. L'onglet actif de signature sur l'IME/IDM est affiché dans cette image.

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



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.