Comment vérifier les changements de comportement dans les signatures IPS après la mise à jour d'un nouveau package de signatures

Contenu

Introduction

Conditions préalables

Conditions requises

Components Used

Problème

Solution

Discussions connexes de la communauté d'assistance Cisco

Introduction

Ce document décrit les changements de comportement introduits par les nouvelles signatures après la mise à jour de Cisco Intrusion Prevention System (IPS) vers un nouveau package de signatures.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Fonctionnalité de mise à jour des signatures sur IPS

Components Used

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

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

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 peut y avoir plusieurs problèmes tels que les pertes de paquets et les problèmes de connectivité avec certaines applications après avoir effectué une mise à jour de signature sur le système IPS.Pour résoudre de tels problèmes, il serait très utile de comprendre les modifications apportées au jeu de signatures actif après la mise à jour de signature.

Solution

Étape 1.

La première chose à vérifier est l'historique de mise à niveau de la signature. Ceci indique le pack de signatures précédent qui était exécuté sur IPS et la version actuelle du pack de signatures.

Ceci peut être trouvé à partir de la sortie de la commande **show version** ou de la section historique de mise à niveau de **show tech**. Un extrait de ce même document est mentionné ici :

Historique des mises à niveau

* IPS-sig-S733-req-E4 19:59:50 UTC 1er août 2015

IPS-sig-S734-req-E4.pkg 19:59:49 UTC jusqu'au 13 août 2015

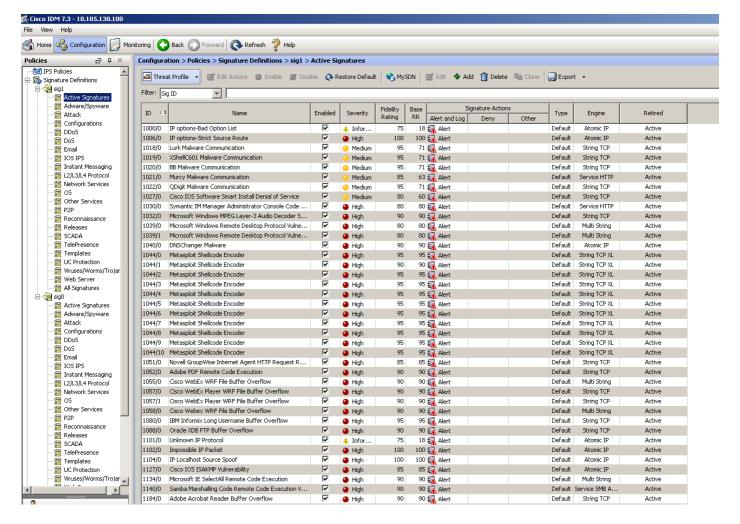
Maintenant, vous pouvez constater que le pack de signatures précédent qui était exécuté sur l'IPS était s733 et a été mis à niveau vers s734, qui est le pack de signatures actuel.

Étape 2.

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

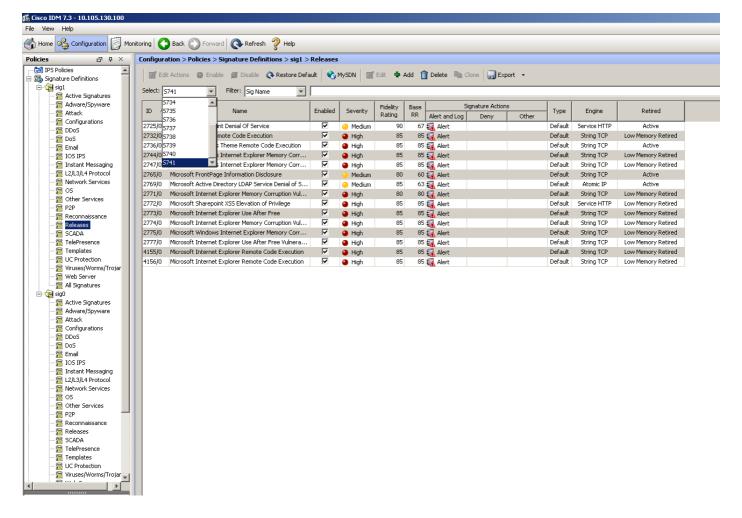
1. L'onglet Signature active de l'IME/IDM est affiché dans cette image.

Accédez à Configuration > Policies > Signature Definitions > Sig1 > Active Signatures.



2. Cette image montre comment sélectionner une version de signature spécifique.

Accédez à Configuration > Policies > Signature Definitions > Sig1 > Release.



En utilisant l'option de filtre que vous avez obtenu toutes les signatures d'une version particulière, vous pouvez les filtrer en fonction du moteur, de la fidélité, de la gravité, etc.

Ce faisant, vous devez être en mesure de vous concentrer sur les modifications apportées à la version des signatures qui peuvent être une cause potentielle du problème en fonction duquel vous alignez votre dépannage.