Come controllare le modifiche comportamentali nelle firme IPS dopo l'aggiornamento di un nuovo pacchetto di firma

Sommario

Introduzione

Questo documento descrive le modifiche comportamentali introdotte dalle nuove firme dopo l'aggiornamento di Cisco Intrusion Prevention System (IPS) a un nuovo pacchetto di firme.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Funzione di aggiornamento della firma su IPS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- IPS serie 4XXX Sensori
- ASA serie 5585-X IPS SSP
- ASA serie 5500-X IPS SSP
- ASA serie 5500 IPS SM

Versione 7.1(10)E4

Versione 7.3(4)E4

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Problema

Dopo aver eseguito un aggiornamento della firma sull'IPS potrebbero verificarsi più problemi, ad esempio perdite di pacchetti e problemi di connettività con alcune applicazioni.Per risolvere questi problemi, è consigliabile comprendere le modifiche apportate al set di firme attivo dopo l'aggiornamento della firma.

Soluzione

Passaggio 1.

La prima cosa da controllare è la cronologia degli aggiornamenti per la firma. In questo modo viene indicato il pacchetto di firma precedente in esecuzione su IPS e la versione corrente del pacchetto di firma.

Questa condizione può essere rilevata dall'output del comando **show version** o dalla sezione upgrade history di **show tech**. Uno snippet della stessa voce è menzionato di seguito:

Cronologia aggiornamenti

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

IPS-sig-S734-req-E4.pkg 19:59:49 UTC mar 13 ago 2015

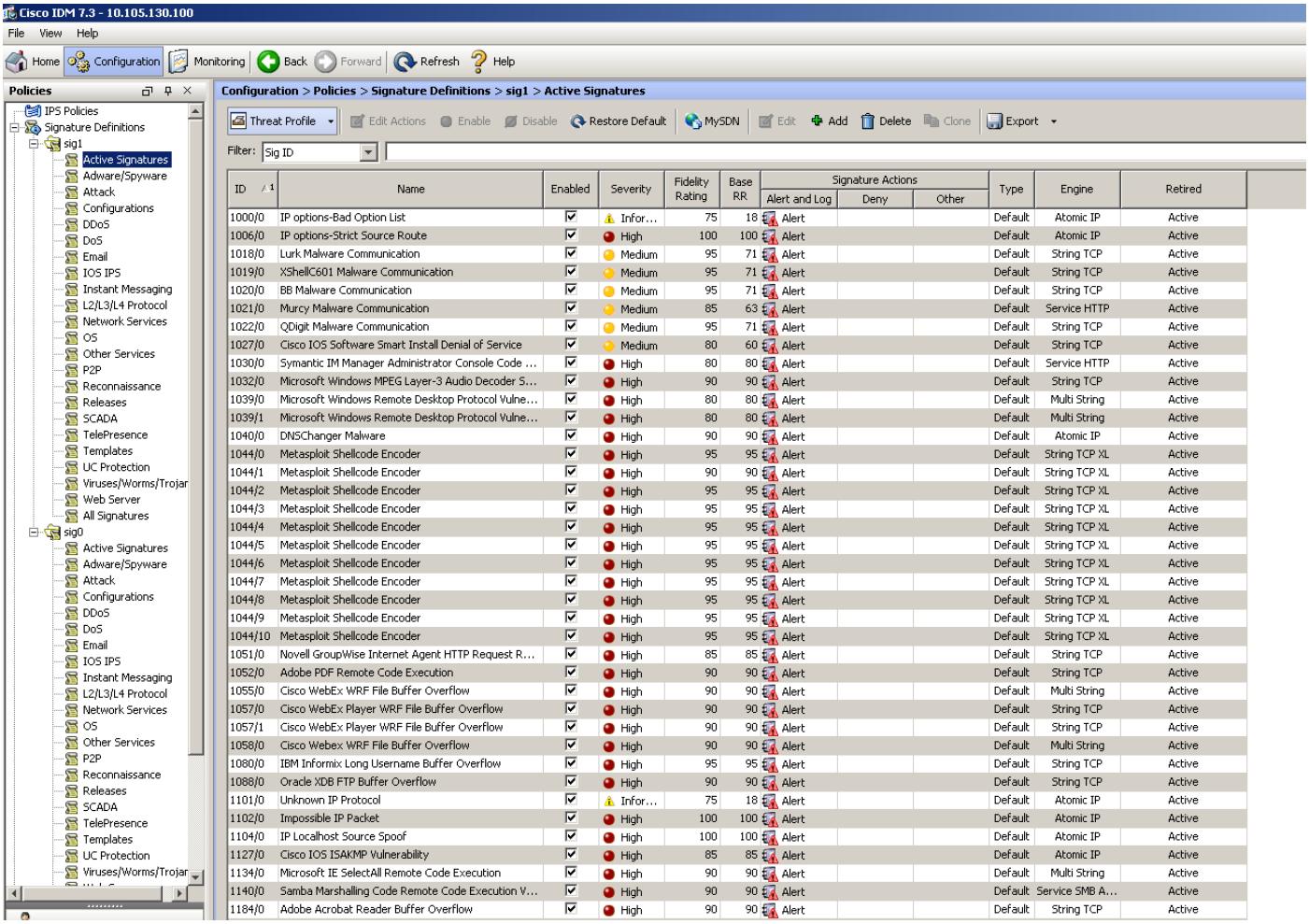
Ora è possibile notare che il precedente pacchetto di firma in esecuzione sull'IPS era s733 ed è stato aggiornato a s734 che è il pacchetto di firma corrente.

Passaggio 2.

Il secondo passaggio consiste nel comprendere le modifiche apportate che possono essere verificate tramite IME/IDM.

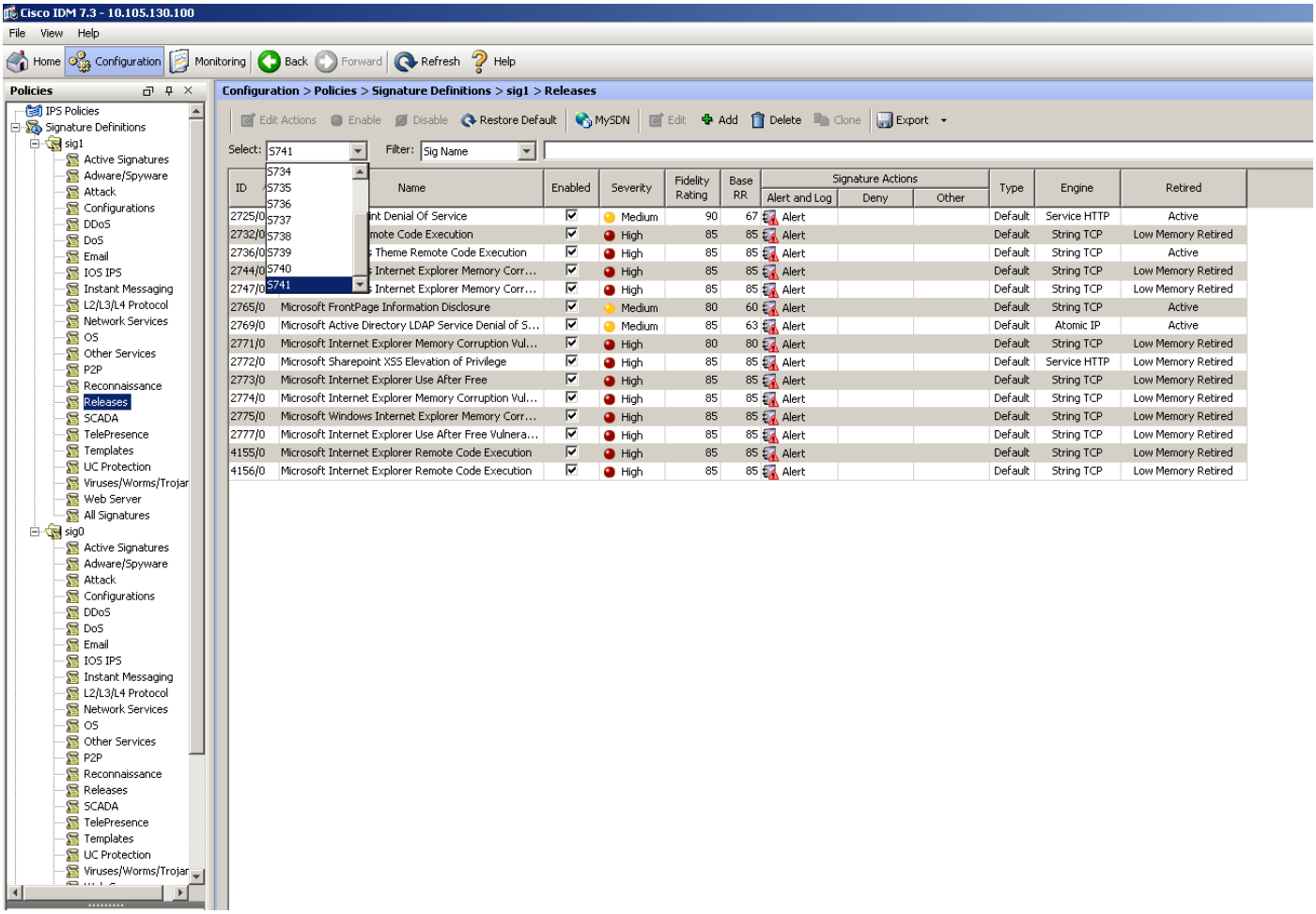
1. In questa immagine viene visualizzata la scheda della firma attiva dell'IME/IDM.

   Selezionare **Configurazione > Criteri > Definizioni firme > Sig1 > Firme attive.**



2. Nell'immagine viene mostrato come selezionare una versione della firma specifica.

Selezionare **Configurazione > Criteri > Definizioni firme > Sig1 > Rilasci.**



Inoltre, utilizzando l'opzione di filtro che avete ottenuto tutte le firme da una particolare release, potete filtrarle in base al motore, alla fedeltà, alla gravità e così via.

In questo modo, è necessario essere in grado di limitare le modifiche alla versione della firma che possono essere una potenziale causa del problema in base al quale allineare la risoluzione dei problemi.