Überprüfung von Verhaltensänderungen in IPS-Signaturen nach der Aktualisierung eines neuen Signaturpakets

Inhalt

Einführung

Dieses Dokument beschreibt die Verhaltensänderungen, die durch die neuen Signaturen nach der Aktualisierung des Cisco Intrusion Prevention System (IPS) auf ein neues Signaturpaket eingeführt wurden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Funktion zur Signaturaktualisierung auf IPS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Sensoren der Serie IPS 4XXX
- ASA 5585-X IPS SSP-Serie
- ASA 5500-X IPS SSP-Serie
- ASA 5500 IPS SSM-Serie

Version 7.1(10)E4

Version 7.3(4)E4

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Problem

Nach der Ausführung eines Signaturaktualisierungvorgangs auf dem IPS kann es mehrere Probleme wie Paketverluste und Verbindungsprobleme bei bestimmten Anwendungen geben.Zur Behebung solcher Probleme ist es sehr hilfreich, wenn Sie die Änderungen beim aktiven Signatursatz nach dem Signaturupdate verstehen.

Lösung

Schritt 1:

Zunächst müssen Sie den Aktualisierungsverlauf für die Signatur überprüfen. Dies zeigt das vorherige Signaturpaket, das auf IPS ausgeführt wurde, und die aktuelle Version des Signaturpakets.

Dies ist in der Ausgabe des Befehls **show version** oder im Abschnitt Upgrade history des **show tech** ersichtlich. Ein Ausschnitt aus diesem Beispiel wird hier erwähnt:

Upgrade-Verlauf

*** IPS-sig-S733-req-E4 19:59:50 UTC Freitag, 09. August 2015**

IPS-sig-S734-req-E4,pkg 19:59:49 UTC Dienstag, 13. August 2015

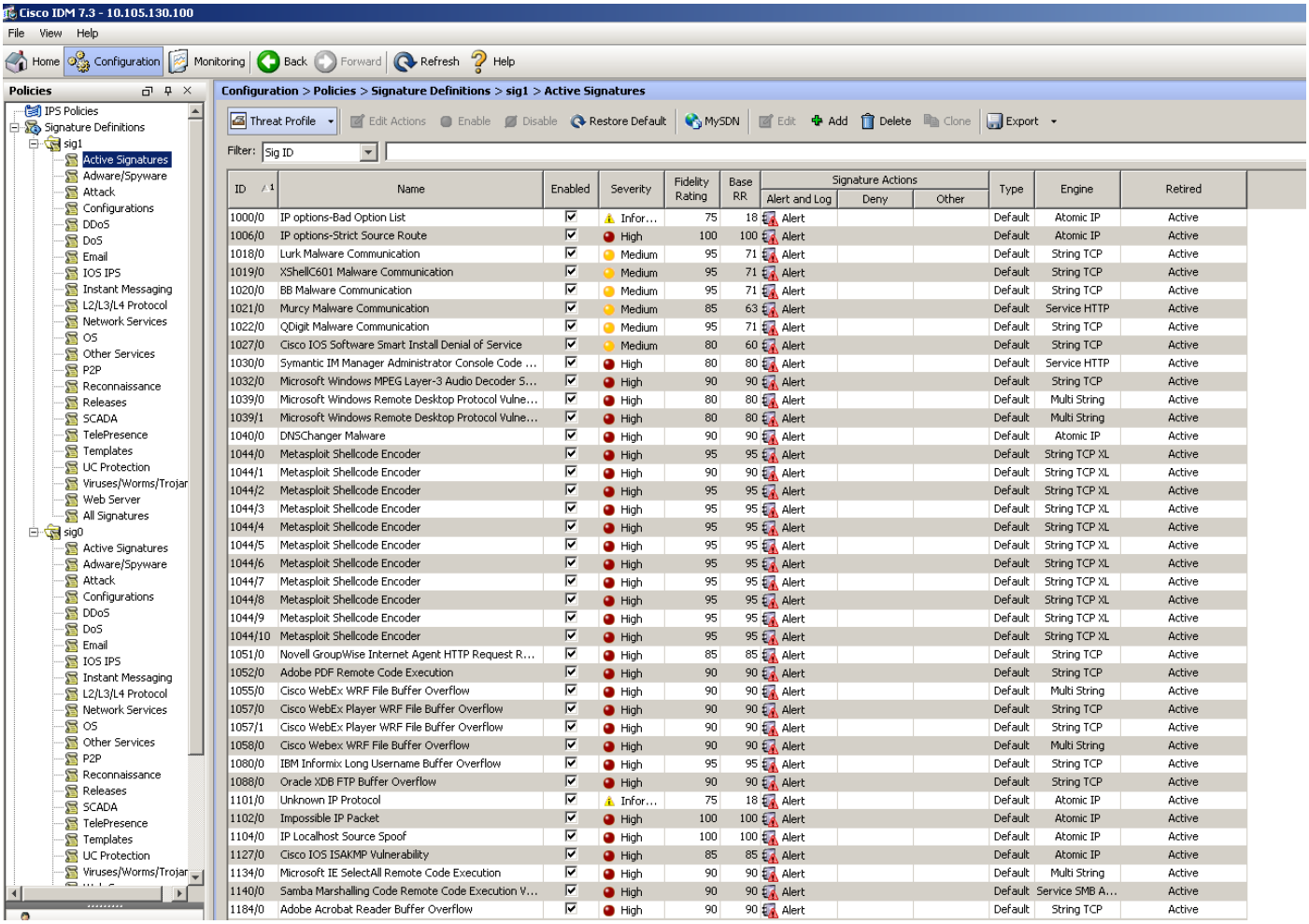
Jetzt können Sie herausfinden, dass das vorherige Signaturpaket, das auf dem IPS ausgeführt wurde, s733 war und auf s734 aktualisiert wurde, das aktuelle Signaturpaket.

Schritt 2:

Der zweite Schritt besteht darin, die vorgenommenen Änderungen zu verstehen, die über IME/IDM überprüft werden können.

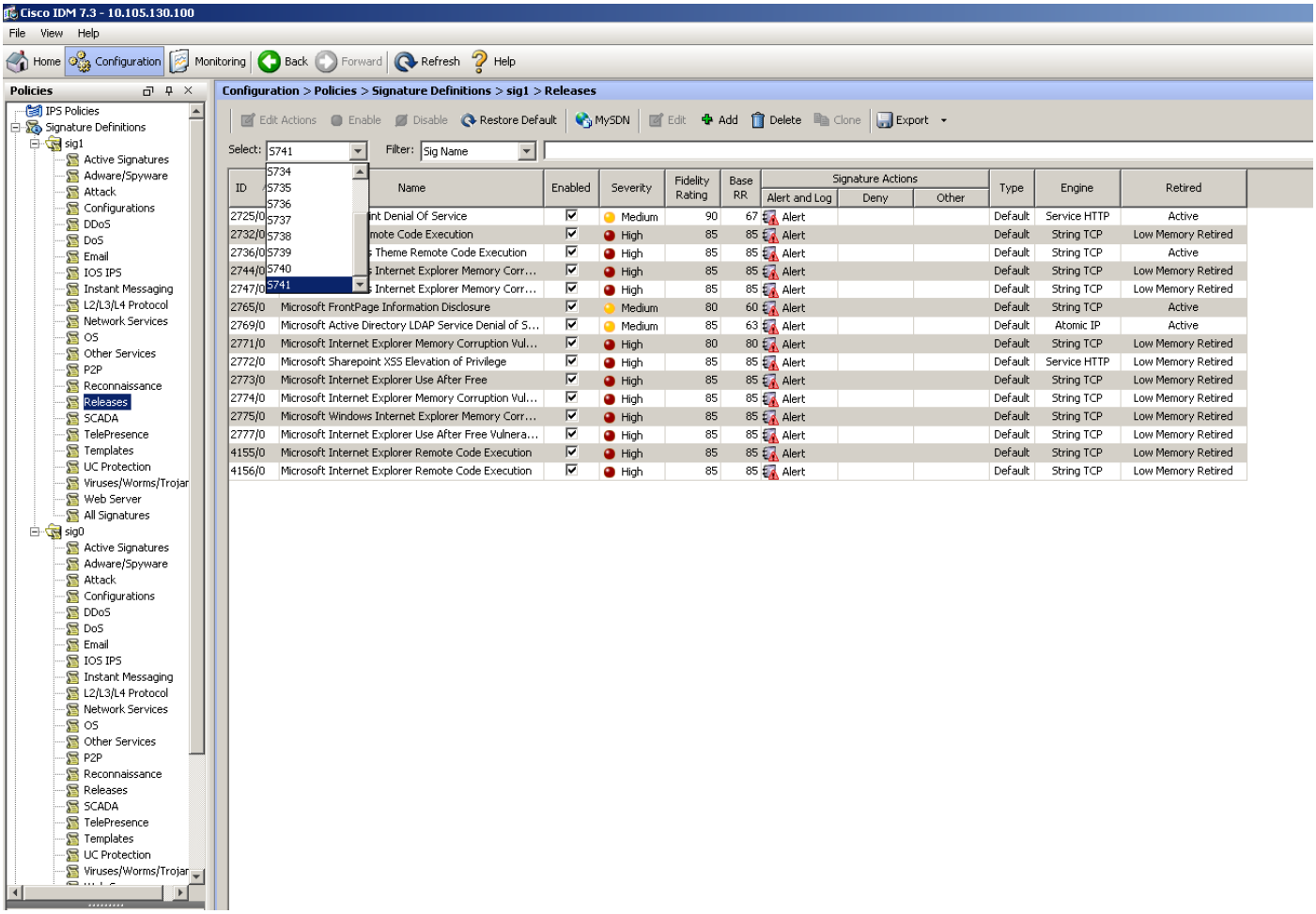
1. In diesem Bild wird die Registerkarte für die aktive Signatur des IME/IDM angezeigt.

Navigieren Sie zu **Konfiguration > Richtlinien > Signaturdefinitionen > Signature1 > Aktive Signaturen.**



2. Dieses Bild zeigt, wie Sie eine bestimmte Signaturversion auswählen.

Navigieren Sie zu **Configuration > Policies > Signature Definitions > Sig1 > Releases.**



Über die Filteroption, die Sie alle Signaturen einer bestimmten Version erhalten haben, können Sie diese nach Engine, Treue, Schweregrad usw. filtern.

Dadurch müssen Sie in der Lage sein, Änderungen in der Signaturversion einzugrenzen, die eine potenzielle Ursache für das Problem sein können, auf dessen Grundlage Sie Ihre Fehlerbehebung abstimmen.