

# 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 > Politiques > Signature Definitions > Sig1 > Active Signatures**.

Cisco IDM 7.3 - 10.105.130.100

File View Help

Home Configuration Monitoring Back Forward Refresh Help

Policies Configuration > Policies > Signature Definitions > sig1 > Active Signatures

Threat Profile Edit Actions Enable Disable Restore Default MySDN Edit Add Delete Clone Export

Filter: Sig ID

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Alert and Log	Deny	Other	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
1018/0	Lurk Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	Alert			Default	String TCP	Active
1019/0	XShellC601 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	QDigit 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	Symantec TM Manager Administrator Console Code ...	<input checked="" type="checkbox"/>	High	80	80	Alert			Default	Service HTTP	Active
1032/0	Microsoft Windows MPEG Layer-3 Audio Decoder S...	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	String TCP	Active
1039/0	Microsoft Windows Remote Desktop Protocol Vulne...	<input checked="" type="checkbox"/>	High	80	80	Alert			Default	Multi String	Active
1039/1	Microsoft Windows Remote Desktop Protocol Vulne...	<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
1104/0	IP Localhost Source Spoof	<input checked="" type="checkbox"/>	High	100	100	Alert			Default	Atomic IP	Active
1127/0	Cisco IOS ISAKMP Vulnerability	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	Atomic IP	Active
1134/0	Microsoft IE SelectAll 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 montre comment sélectionner une version de signature spécifique.

Accédez à **Configuration > Politiques > Signature Definitions > Sig1 > Release.**

Cisco IDM 7.3 - 10.105.130.100

File View Help

Home Configuration Monitoring Back Forward Refresh Help

Policies Configuration > Policies > Signature Definitions > sig1 > Releases

Select: 5741 Filter: Sig Name

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions			Type	Engine	Retired
						Alert and Log	Deny	Other			
2725/0	Denial Of Service	<input checked="" type="checkbox"/>	Medium	90	67	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Service HTTP	Active
2732/0	Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2736/0	Theme Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
2744/0	Internet Explorer Memory Cor...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2747/0	Internet Explorer Memory Corr...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2765/0	Microsoft FrontPage Information Disclosure	<input checked="" type="checkbox"/>	Medium	80	60	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
2769/0	Microsoft Active Directory LDAP Service Denial of S...	<input checked="" type="checkbox"/>	Medium	85	63	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Atomic IP	Active
2771/0	Microsoft Internet Explorer Memory Corruption Vul...	<input checked="" type="checkbox"/>	High	80	80	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2772/0	Microsoft Sharepoint XSS Elevation of Privilege	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Service HTTP	Low Memory Retired
2773/0	Microsoft Internet Explorer Use After Free	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2774/0	Microsoft Internet Explorer Memory Corruption Vul...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2775/0	Microsoft Windows Internet Explorer Memory Corr...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2777/0	Microsoft Internet Explorer Use After Free Vulnera...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
4155/0	Microsoft Internet Explorer Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
4156/0	Microsoft Internet Explorer Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired

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.