

Hoe gedragsveranderingen in IPS-handtekeningen te controleren Post met een nieuw handtekeningen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

[Gerelateerde Cisco Support Community-discussies](#)

Inleiding

Dit document beschrijft de gedragsveranderingen die door de nieuwe handtekeningen zijn geïntroduceerd na het uploaden van Cisco Inbraakpreventiesysteem (IPS) naar een nieuw pakket handtekeningen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Functie voor bijwerken van handtekeningen op IPS

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- IPS 4XXX Series sensoren
- ASA 5585-X IPS SSP-serie
- ASA 5500-X IPS SSP-Series Next-Generation
- ASA 5500 IPS IPS SM-serie

versie 7.1(10)E4

Versie 7.3(4)E4

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

Probleem

Er zouden meerdere problemen kunnen zijn zoals pakketdruppels en aansluitingsproblemen met bepaalde toepassingen na het uitvoeren van een signatuur update op de IPS. Om dergelijke problemen op te lossen zou het zeer behulpzaam zijn als u de veranderingen in actieve signatuur kunt begrijpen die plaatste post van de signatuur update.

Oplossing

Stap 1.

Het eerste wat je moet controleren is de upgradegeschiedenis voor de handtekening. Dit vertelt het vorige handboekenpakket dat op IPS actief was en de huidige versie van handboekenpakket.

Dit kan worden gevonden in de output van de **opdrachtshow versie** of in het upgradeoverzicht van de **showtechnologie**. Snippet van hetzelfde onderwerp wordt hier genoemd:

Upgradegeschiedenis

*** IPS-sig-S733-req-E4 19:59:50 UTC FRJ augustus 2015**

IPS-sig-S734-req-E4.pkg 19:59:49 UTC Tue 13 augustus 2015

Nu kunt u duidelijk maken dat het vorige signatuur-pakket dat op IPS liep s733 was en opgewaardeerd werd tot s734, wat het huidige handboekje is.

Stap 2.

De tweede stap is het begrijpen van de veranderingen die zijn aangebracht en die kunnen worden gecontroleerd via de IME/IDM.

1. Het tabblad actieve handtekening op IME/IDM wordt in deze afbeelding weergegeven.

Navigeer naar **Configuration > Policy > 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	Symantic 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. Deze afbeelding toont hoe een specifieke handmatige release moet worden geselecteerd.

Navigeer naar **Configuratie > Beleid > Definities voor handtekeningen > Sig1 > releases**.

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

Als u verder de filteroptie gebruikt die u hebt aangeschaft, kunt u alle handtekeningen bij een bepaalde release filteren op basis van motor, trouw, ernst, enz.

Door dit te doen moet u in staat zijn om af te remmen op de veranderingen in de handmatige release die een mogelijke oorzaak voor de kwestie kan zijn op basis waarvan u de probleemoplossing uitlijnen.