

# IPS 시그니처의 동작 변경 확인 새 서명 패키지 업데이트 후 확인 방법

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[문제](#)

[솔루션](#)

[관련 Cisco 지원 커뮤니티 토론](#)

## 소개

이 문서에서는 Cisco IPS(Intrusion Prevention System)를 새 서명 패키지로 업데이트한 후 새로운 서명에 의해 도입된 동작 변화에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IPS의 시그니처 업데이트 기능

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IPS 4XXX 시리즈 센서
- ASA 5585-X IPS SSP 시리즈
- ASA 5500-X IPS SSP 시리즈
- ASA 5500 IPS SSM 시리즈

버전 7.1(10)E4

버전 7.3(4)E4

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

## 문제

IPS에서 시그니처 업데이트를 수행한 후 패킷 삭제 및 특정 애플리케이션에 대한 연결 문제와 같은 여러 문제가 발생할 수 있습니다. 이러한 문제를 해결하려면 서명 업데이트 후 활성화 서명 세트의 번

경 사항을 이해할 수 있으면 매우 유용합니다.

## 솔루션

### 1단계.

먼저 시그니처의 업그레이드 기록을 확인해야 합니다. IPS에서 실행 중인 이전 시그니처 팩과 현재 버전의 시그니처 팩이 표시됩니다.

이 정보는 명령 **show version**의 출력이나 **show tech**의 업그레이드 기록 섹션에서 확인할 수 있습니다. 동일한 항목의 코드 조각은 다음과 같습니다.

업그레이드 기록

**\* IPS-sig-S733-req-E4 19:59:50 UTC 2015년 8월 9일 금요일**

**IPS-sig-S734-req-E4.pkg 19:59:49 UTC 화 2015년 8월 13일**

이제 IPS에서 실행 중이던 이전 서명 팩이 s733이고 현재 서명 팩인 s734로 업그레이드되었음을 확인할 수 있습니다.

### 2단계.

두 번째 단계는 IME/IDM을 통해 확인할 수 있는 변경 사항을 이해하는 것입니다.

1. IME/IDM의 활성 서명 탭이 이 이미지에 표시됩니다.

Configuration(컨피그레이션) > Policies(정책) > Signature Definitions(시그니처 정의) > Sig1 > Active Signatures(활성 시그니처)로 이동합니다.

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. 이 이미지는 특정 서명 릴리스를 선택하는 방법을 보여줍니다.

Configuration(컨피그레이션) > Policies(정책) > Signature Definitions(시그니처 정의) > Sig1 > Releases(릴리스)로 이동합니다.

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

특정 릴리스에서 모든 시그니처를 얻은 필터 옵션을 사용하여 엔진, 정확도, 심각도 등을 기준으로 필터링할 수 있습니다.

이를 통해 문제 해결을 조율하는 데 따라 문제의 잠재적 원인이 될 수 있는 서명 릴리스의 변경 사항을 좁힐 수 있어야 합니다.