

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题](#)

[解决方案](#)

[相关的思科支持社区讨论](#)

简介

本文描述新的签名介绍的性能上的更改在更新思科入侵防御系统以后(IPS)到一个新的签名包。

先决条件

要求

Cisco 建议您了解以下主题：

- 在IPS的签名更新功能

使用的组件

本文档中的信息基于以下软件和硬件版本：

- IPS 4XXX系列传感器
- ASA 5585-X IPS SSP系列
- ASA 5500-X IPS SSP系列
- ASA 5500 IPS SSM系列

版本7.1(10)E4

版本7.3(4)E4

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

问题

可能有多问题例如丢包，并且与某些应用程序的连通性问题，在执行在IPS.To后的一次签名更新排除故障是非常有用的这样问题，如果能了解在设置的活动签名上的变化张贴签名更新。

解决方案

步骤1:

您需要检查的第一件事是签名的升级历史记录。这告诉在IPS和签名装箱当前版本运行的上一个签名装箱。

这可以从show version命令的输出发现或从升级显示tech.片断的History部分从同样的被提及在这儿：

升级历史记录

* IPS-sig-S733-req-E4 19:59:50 UTC星期五八月09 2015

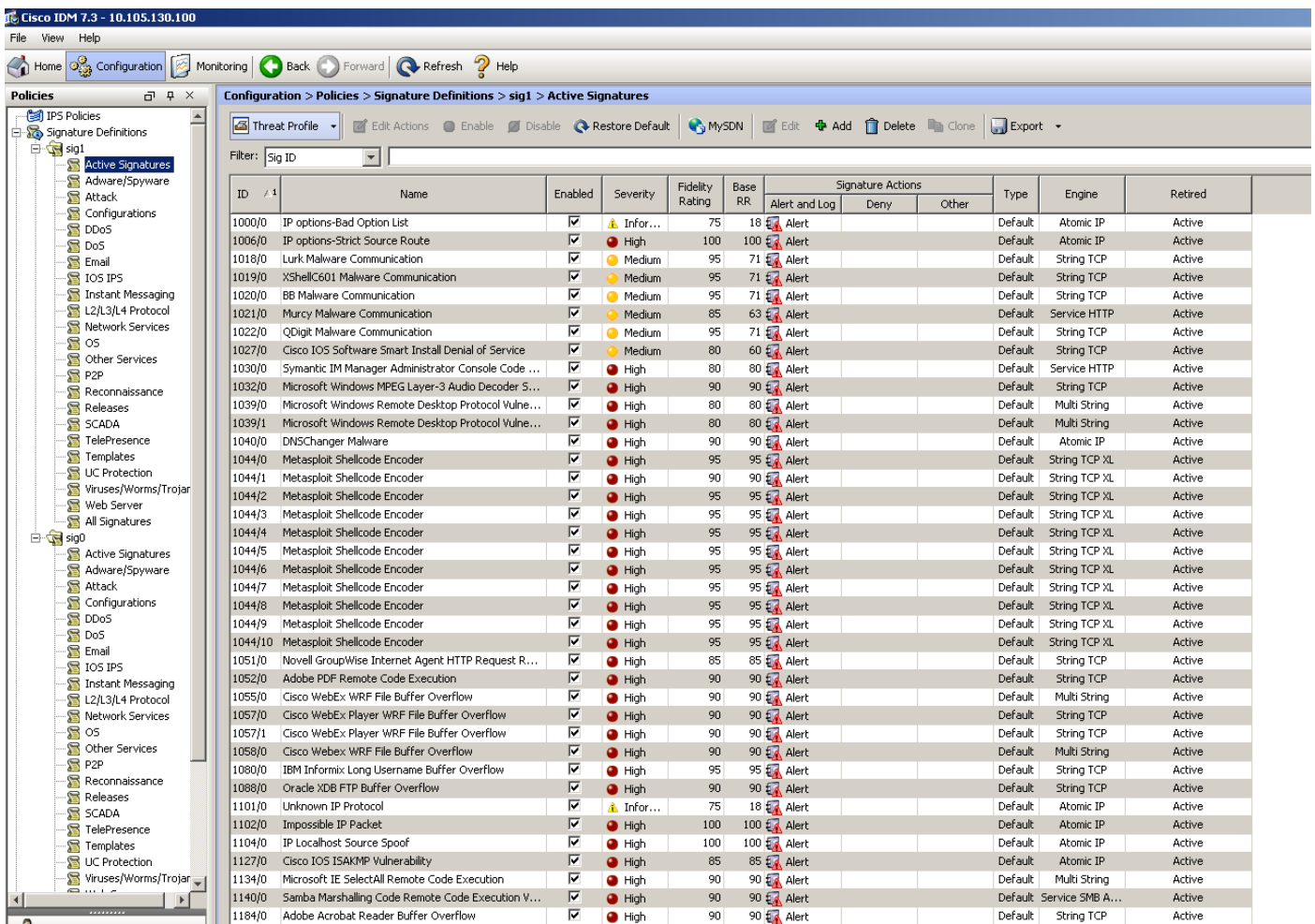
现在您能做在IPS运行的上一个签名装箱是s733和升级对是当前签名装箱的s734。

第二步：

第二步将了解做了，并且可以通过IME/IDM被检查的变动。

1. 在IME/IDM的活动签名选项卡在此镜像显示。

导航对Configuration>策略>签名定义> Sig1 >活动签名。



ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions			Type	Engine	Retired
						Alert and Log	Deny	Other			
1000/0	IP options-Bad Option List	<input checked="" type="checkbox"/>	Inform...	75	18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Atomic IP	Active
1006/0	IP options-Strict Source Route	<input checked="" type="checkbox"/>	High	100	100	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Atomic IP	Active
1018/0	Lurk Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1019/0	XShellC601 Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1020/0	BB Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1021/0	Murcy Malware Communication	<input checked="" type="checkbox"/>	Medium	85	63	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Service HTTP	Active
1022/0	QDigit Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1027/0	Cisco IOS Software Smart Install Denial of Service	<input checked="" type="checkbox"/>	Medium	80	60	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1030/0	Symantec IM Manager Administrator Console Code ...	<input checked="" type="checkbox"/>	High	80	80	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Service HTTP	Active
1032/0	Microsoft Windows MPEG Layer-3 Audio Decoder S...	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1039/0	Microsoft Windows Remote Desktop Protocol Vulne...	<input checked="" type="checkbox"/>	High	80	80	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Multi String	Active
1039/1	Microsoft Windows Remote Desktop Protocol Vulne...	<input checked="" type="checkbox"/>	High	80	80	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Multi String	Active
1040/0	DNSChanger Malware	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Atomic IP	Active
1044/0	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/1	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/2	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/3	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/4	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/5	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/6	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/7	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/8	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/9	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1044/10	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP XL	Active
1051/0	Novell GroupWise Internet Agent HTTP Request R...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1052/0	Adobe PDF Remote Code Execution	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1055/0	Cisco WebEx WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Multi String	Active
1057/0	Cisco WebEx Player WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1057/1	Cisco WebEx Player WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1058/0	Cisco Webex WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Multi String	Active
1080/0	IBM Informix Long Username Buffer Overflow	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1088/0	Oracle XDB FTP Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
1101/0	Unknown IP Protocol	<input checked="" type="checkbox"/>	Inform...	75	18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Atomic IP	Active
1102/0	Impossible IP Packet	<input checked="" type="checkbox"/>	High	100	100	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Atomic IP	Active
1104/0	IP Localhost Source Spoof	<input checked="" type="checkbox"/>	High	100	100	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Atomic IP	Active
1127/0	Cisco IOS ISAKMP Vulnerability	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Atomic IP	Active
1134/0	Microsoft IE SelectAll Remote Code Execution	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Multi String	Active
1140/0	Samba Marshalling Code Remote Code Execution V...	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Service SMB A...	Active
1184/0	Adobe Acrobat Reader Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active

2. 此镜像显示如何选择一特定签名版本。

导航到Configuration>策略>签名定义> Sig1 >版本。

促进使用您从一特定的版本获取所有签名的过滤器选项，您能过滤他们根据引擎、保真度，严重性

等。

通过该执行您在可以是根据的签名版本上的变化一定能缩小哪些问题的一潜在原因您对齐您的故障排除。