

如何在更新新签名包后检查IPS签名中的行为更改

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

本文档介绍将思科入侵防御系统(IPS)更新到新签名包后新签名引入的行为更改。

先决条件

要求

Cisco 建议您了解以下主题：

- IPS上的签名更新功能

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

在IPS上执行签名更新后，可能会出现多个问题，例如丢包和某些应用程序的连接问题。要解决此类问题，请务必了解签名更新后活动签名集中的更改。

解决方案

步骤1:

您首先需要检查签名的升级历史记录。这将告知在IPS上运行的以前的签名包和当前版本的签名包。

这可以从命令show version的输出或从show tech的升级历史记录部分中找到。此处提到了同一命令的代码片段：

升级历史记录

* IPS-sig-S733-req-E4 19:59:50 UTC星期五2015年8月09日

IPS-sig-S734-req-E4.pkg 19:59:49 UTC周二8月13日2015

现在，您可以确定在IPS上运行的以前的签名包是s733，并已升级到s734，这是当前的签名包。

第二步：

第二步是了解已进行的更改，以及可通过IME/IDM检查的更改。

1. IME/IDM上的活动签名选项卡显示在此图像中。

导航至Configuration > Policies > Signature Definitions > Sig1 > Active Signatures。

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"/>	Informational	75	18	<input checked="" type="checkbox"/>			Default	Atomic IP	Active
1006/0	IP options-Strict Source Route	<input checked="" type="checkbox"/>	High	100	100	<input checked="" type="checkbox"/>			Default	Atomic IP	Active
1018/0	Lurk Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	<input checked="" type="checkbox"/>			Default	String TCP	Active
1019/0	XShellC601 Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	<input checked="" type="checkbox"/>			Default	String TCP	Active
1020/0	BB Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	<input checked="" type="checkbox"/>			Default	String TCP	Active
1021/0	Murcy Malware Communication	<input checked="" type="checkbox"/>	Medium	85	63	<input checked="" type="checkbox"/>			Default	Service HTTP	Active
1022/0	QDigit Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	<input checked="" 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"/>			Default	String TCP	Active
1030/0	Symantic IM Manager Administrator Console Code ...	<input checked="" type="checkbox"/>	High	80	80	<input checked="" 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"/>			Default	String TCP	Active
1039/0	Microsoft Windows Remote Desktop Protocol Vulne...	<input checked="" type="checkbox"/>	High	80	80	<input checked="" 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"/>			Default	Multi String	Active
1040/0	DNSChanger Malware	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>			Default	Atomic IP	Active
1044/0	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/1	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/2	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/3	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/4	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/5	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/6	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/7	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/8	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/9	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" type="checkbox"/>			Default	String TCP XL	Active
1044/10	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	<input checked="" 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"/>			Default	String TCP	Active
1052/0	Adobe PDF Remote Code Execution	<input checked="" type="checkbox"/>	High	90	90	<input checked="" 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"/>			Default	Multi String	Active
1057/0	Cisco WebEx Player WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	<input checked="" 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"/>			Default	String TCP	Active
1058/0	Cisco WebEx WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	<input checked="" 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"/>			Default	String TCP	Active
1088/0	Oracle XDB FTP Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	<input checked="" type="checkbox"/>			Default	String TCP	Active
1101/0	Unknown IP Protocol	<input checked="" type="checkbox"/>	Informational	75	18	<input checked="" type="checkbox"/>			Default	Atomic IP	Active
1102/0	Impossible IP Packet	<input checked="" type="checkbox"/>	High	100	100	<input checked="" type="checkbox"/>			Default	Atomic IP	Active
1104/0	IP Localhost Source Spoof	<input checked="" type="checkbox"/>	High	100	100	<input checked="" type="checkbox"/>			Default	Atomic IP	Active
1127/0	Cisco IOS ISAKMP Vulnerability	<input checked="" type="checkbox"/>	High	85	85	<input checked="" 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"/>			Default	Multi String	Active
1140/0	Samba Marshalling Code Remote Code Execution V...	<input checked="" type="checkbox"/>	High	90	90	<input checked="" 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"/>			Default	String TCP	Active

2.此图显示如何选择特定签名版本。

导航至 Configuration > Policies > Signature Definitions > Sig1 > Releases.

The screenshot shows the Cisco IDM 7.3 web interface. The breadcrumb navigation is Configuration > Policies > Signature Definitions > sig1 > Releases. The left sidebar shows a tree view of policies, with 'Releases' selected under 'sig1'. The main area displays a table of signature releases with the following columns: ID, Name, Enabled, Severity, Fidelity Rating, Base RR, Signature Actions (Alert and Log, Deny, Other), Type, Engine, and Retired.

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions			Type	Engine	Retired
						Alert and Log	Deny	Other			
5734											
2725/0	Denial Of Service	<input checked="" type="checkbox"/>	Medium	90	67	Alert			Default	Service HTTP	Active
2732/0	Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Low Memory Retired
2736/0	Theme Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Active
2744/0	Internet Explorer Memory Cor...	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Low Memory Retired
2747/0	Internet Explorer Memory Cor...	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Low Memory Retired
2765/0	Microsoft FrontPage Information Disclosure	<input checked="" type="checkbox"/>	Medium	80	60	Alert			Default	String TCP	Active
2769/0	Microsoft Active Directory LDAP Service Denial of S...	<input checked="" type="checkbox"/>	Medium	85	63	Alert			Default	Atomic IP	Active
2771/0	Microsoft Internet Explorer Memory Corruption Vul...	<input checked="" type="checkbox"/>	High	80	80	Alert			Default	String TCP	Low Memory Retired
2772/0	Microsoft Sharepoint XSS Elevation of Privilege	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	Service HTTP	Low Memory Retired
2773/0	Microsoft Internet Explorer Use After Free	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Low Memory Retired
2774/0	Microsoft Internet Explorer Memory Corruption Vul...	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Low Memory Retired
2775/0	Microsoft Windows Internet Explorer Memory Cor...	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Low Memory Retired
2777/0	Microsoft Internet Explorer Use After Free Vulnera...	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Low Memory Retired
4155/0	Microsoft Internet Explorer Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Low Memory Retired
4156/0	Microsoft Internet Explorer Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Low Memory Retired

进一步，使用过滤器选项，您可以根据引擎、保真度、严重性等来过滤从特定版本获取的所有签名

。

通过这样做，您必须能够缩小签名版本中的更改范围，这些更改可能会根据您调整故障排除的原因导致问题。