如何在更新新签名包后检查IPS签名中的行为更改

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 问题 <u>解决方案</u> 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 <u>Cisco 技术提示规则。</u>

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。

File View Help											
🖏 Home 🦓 Configuration 📴 Monitoring 💽 Back 🕥 Forward 🔊 Refresh 🦻 Help											
Policies P × Configuration > Policies > Signature Definitions > sig1 > Active Signatures											
PS Policies											
🕂 💫 Signature Definitions 🔰 🖾 Threat Profile 🔹 🖉 Edit Actions 🕒 Enable 🖉 Disable 🖉 Restore Default 🥎 MySDN 🖉 Edit 🍄 Add 😈 Delete 🐃 Clone 🕁 Export 🔹											
-Se Active Signatures											
To Advance/Spyware D. / 1 Name Enabled Severity Fidelity Base Signature Actions Type Engine D	etired										
Configuration	ourou										
- State Configurations and Configuration of the American State Sta	active										
💦 DoS 1006/0 IP options-Strict Source Route 🔽 🥥 High 100 100 🏭 Alert Default Atomic IP	Active										
- 🚡 Email 1018/0 Lurk Malware Communication 🗹 🥥 Medium 95 71 🌠 Alert Default String TCP	active										
🛛 🖉 IOS IPS 🔹 1019/0 XShellC601 Malware Communication 🔽 🥥 Medium 95 71 🏭 Alert Default String TCP	Active										
- 📓 Instant Messaging 🔰 1020/0 BB Malware Communication 🔽 🥥 Medium 95 71 🌠 Alert Default String TCP	ictive										
- 🔀 L2[L3]L4 Protocol 🔰 1021/0 Murcy Malware Communication 🔽 🧿 Medium 85 63 🚮 Alert Default Service HTTP	Active										
Network Services 1022/0 QDigit Malware Communication 🗹 🥥 Medium 95 71 🏭 Alert Default String TCP	sctive										
🛛 🖓 05 0 Medium 80 60 🌠 Alert 🛛 Default String TCP	Active										
🔐 Outer Service MTTP and Service MTTP a	sctive										
🛛 🔤 Reconnaissance 🔹 1032/0 Microsoft Windows MPEG Layer-3 Audio Decoder S 🔽 🥥 High 90 90 🏹 Alert Default String TCP a	Active										
🔤 📲 🔤 👘 👘 👘 🖓 👘 🖓 👘 🖓 👘 🖓 👘 🖓 👘 🖓 👘 🖓 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘	sctive										
🔤 🔤 SCADA 🔰 1039/1 Microsoft Windows Remote Desktop Protocol Vulne 🔽 🥥 High 80 80 🏭 Alert Default Multi String	Active										
- 🛜 TelePresence 1040/0 DNSChanger Malware 🔽 🕒 High 90 90 🚱 Alert Default Atomic IP	active										
🔚 Templates 🔰 1044/0 Metasploit Shellcode Encoder 🔽 🥥 High 95 95 🏹 Alert Default String TCP XL	Active										
🔚 UC Protection 1044/1 Metasploit Shellcode Encoder 🔽 🕒 High 90 90 🌠 Alert Default String TCP XL	active										
🔽 Vrusses Worms (1 ro)ar 🔰 1044/2 Metasploit Shellcode Encoder 🔽 🕒 High 95 95 🏹 Alert Default String TCP XL	Active										
🔐 web Jak Ven Straht web 1044/3 Metasploit Shellcode Encoder 🔽 🕒 High 95 95 🙀 Alert Default String TCP XL	active										
🖬 m signed et string TCP XL at 1044/4 Metasploit Shellcode Encoder 🔽 🕒 High 95 95 🏭 Alert Default String TCP XL at	sctive										
🔽 Active Signatures 1044/5 Metasploit Shellcode Encoder 🔽 🕒 High 95 95 🙀 Alert Default String TCP XL	active										
🛛 🖳 🖓 dware/Spyware 🔹 1044/6 Metasploit Shellcode Encoder 🛛 🔽 🥥 High 95 95 🌠 Alert Default String TCP XL	Active										
- 🛜 Attack 1044/7 Metasploit Shellcode Encoder 🔽 💽 High 95 95 🙀 Alert Default String TCP XL	active										
🛛 🖓 Configurations 🔹 🔰 1044/8 Metasploit Shellcode Encoder 🛛 🔽 🥥 High 95 95 🌠 Alert Default String TCP XL	Active										
DooS 1044/9 Metasploit Shellcode Encoder 🔽 🕒 High 95 95 🙀 Alert Default String TCP XL	active										
🔤 🖂 UOS 🔤 1044/10 Metasploit Shellcode Encoder 🔽 🥥 High 95 95 🏭 Alert Default String TCP XL 🗤	sctive										
🔚 Einair 1051/0 Novell GroupWise Internet Agent HTTP Request R 🔽 🔮 High 85 85 🙀 Alert Default String TCP and	active										
🔤 Tostan Bessaning 🔰 1052/0 Adobe PDF Remote Code Execution 🔽 🥥 High 90 90 🚱 Alert Default String TCP	Active										
S L2/L3/L4 Protocol 1055/0 Cisco WebEx WRF File Buffer Overflow 🔽 💽 High 90 90 😨 Alert Default Multi String	ctive										
- 🛜 Network Services 🔰 1057/0 Cisco WebEx Player WRF File Buffer Overflow 🔽 🥥 High 90 90 🚱 Alert Default String TCP	Active										
- 🛣 OS 1057/1 Cisco WebEx Player WRF File Buffer Overflow 🔽 🕒 High 90 90 🌠 Alert Default String TCP	active										
📓 Other Services 🔰 1058/0 Cisco Webex WRF File Buffer Overflow 🔽 🥥 High 90 90 🙀 Alert Default Multi String	Active										
📓 P2P 1080/0 IBM Informix Long Username Buffer Overflow 🔽 💽 High 95 95 🙀 Alert Default String TCP	ctive										
Reconnaissance 1088/0 Oracle XDB FTP Buffer Overflow 🔽 🕒 High 90 90 🛃 Alert Default String TCP	Active										
🔐 Kerebases 1101/0 Unknown IP Protocol 🗹 🛦 Infor 75 18 🛃 Alert Default Atomic IP	ctive										
an John TalePreserve 1102/0 Impossible IP Packet 🗸 🖉 🕒 High 100 100 🔂 Alert Default Atomic IP	Active										
- Templates 1104/0 IP Localhost Source Spoof 🔽 🕒 High 100 100 🙀 Alert Default Atomic IP	ctive										
- 👷 UC Protection 1127/0 Cisco IOS ISAKMP Vulnerability 🔽 💽 High 85 85 🛃 Alert Default Atomic IP	Active										
- 🛜 Viruses/Worms/Trojar 🚽 1134/0 Microsoft IE SelectAll Remote Code Execution 🛛 🖉 🕒 High 90 90 🛃 Alert Default Multi String	sctive										
🖌 🛛 📊 🖌 🖌 🖌 🖌 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹	Active										
1184/0 Adobe Acrobat Reader Buffer Overflow 🔽 💁 High 90 90 🙀 Alert Default String TCP	ctive										

2.此图显示如何选择特定签名版本。

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

🕼 Cisco IDM 7.3 - 10.105.130.100												
File View Help												
The Configuration of Monitoring Configuration Back Forward Refresh of Help												
Policies 고무×	X Configuration > Policies > Signature Definitions > sign > Releases											
IPS Policies IPS Policies IPS Signature Definitions IPS signatures												
	5734 A ID 5735 Nam	e Enable	d Severity	Fidelity Rating	Base RR 4	S Alert and Log	ignature Actions Deny	Other	Туре	Engine	Retired	
Configurations	2725/0 5737 Int Denial C	of Service	Medium	90	67 £	Alert			Default	Service HTTP	Active	
DDo5	2732/0 5738 mote Code	Execution 🔽	A High	85	85 £	Alert			Default	String TCP	Low Memory Retired	
C Empil	2736/05739 Theme Re	mote Code Execution	High	85	85 £	Alert			Default	String TCP	Active	
	2744/0 5740 Internet f	Explorer Memory Corr	A High	85	85 £	Alert			Default	String TCP	Low Memory Retired	
S Instant Messaging	2747/0 5741	xplorer Memory Corr	A High	85	85 £	Alert			Default	String TCP	Low Memory Retired	
	2765/0 Microsoft FrontPage Informa	tion Disclosure	Medium	80	60 £	a Alert			Default	String TCP	Active	
	2769/0 Microsoft Active Directory LD	AP Service Denial of S	Medium	85	63 £	Δlert			Default	Atomic IP	Active	
	2771/0 Microsoft Internet Explorer M	lemory Corruption Vul	A High	80	80 £	Alert			Default	String TCP	Low Memory Retired	
	2772/0 Microsoft Sharepoint XSS Elev	vation of Privilege	 High 	85	85 f	A Alert			Default	Service HTTP	Low Memory Retired	
	2773/0 Microsoft Internet Explorer I	se After Free	 High 	85	85 f	1 Alert			Default	String TCP	Low Memory Retired	
	2774/0 Microsoft Internet Explorer N	lemory Corruption Vul	 High 	85	85 f	Allort			Default	String TCP	Low Memory Retired	
	2775/0 Microsoft Windows Internet #	Explorer Memory Corr	 High 	85	85 f	Alert			Default	String TCP	Low Memory Retired	
	2777/0 Microsoft Internet Explorer I	se After Free Vulpera	 High 	85	85 f	A filert			Default	String TCP	Low Memory Retired	
	4155/0 Microsoft Internet Explorer R	emote Code Execution	 High 	85	85 f	Allort			Default	String TCP	Low Memory Retired	
UC Protection	4156/0 Microsoft Internet Explorer R	emote Code Execution	 High 	85	85 f	Alert			Default	String TCP	Low Memory Retired	
	Troopo The sole incomo Explorer in		- riigii	00	00 🖣	Alloi C			Dordaic	Sangra	contributory reduced	
All Signatures												
Active Signatures												
Attack												
Configurations												
DDo5												
IOS IPS												
Instant Messaging												
E2/L3/L4 Protocol												
P2P												
TelePresence												
I emplates												
Viruses/Worms/Trojer												
a widses/worms/froja												

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。