

在更新新特徵碼包後如何檢查IPS特徵碼中的行為更改

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[問題](#)

[解決方案](#)

[相關思科支援社群討論](#)

簡介

本檔案介紹將思科入侵防禦系統(IPS)更新至新特徵碼包後新特徵碼引入的行為變化。

必要條件

需求

思科建議您瞭解以下主題：

- IPS上的特徵碼更新功能

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- IPS 4XXX系列感測器
- 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

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

問題

在IPS上執行特徵碼更新後，某些應用程式可能會出現多種問題，例如丟包和連線問題。若要解決此類問題，如果能夠瞭解在特徵碼更新後活動特徵碼集的更改，將會非常有用。

解決方案

步驟1.

首先需要檢查的是簽名的升級歷史記錄。這將告知在IPS上運行的上一個特徵碼包和當前版本的特徵碼包。

可從show version指令的輸出或show tech的升級歷史記錄部分找到此內容。此處會提到來自相同內容的片段：

升級歷史記錄

* IPS-sig-S733-req-E4 19:59:50 UTC週五2015年8月09日

IPS-sig-S734-req-E4.pkg 19:59:49 UTC週二2015年8月13日

現在，您可以發現IPS上運行的前一個特徵碼包是s733，並且已升級為當前特徵碼包的s734。

步驟2.

第二步是瞭解已經進行的更改以及可以通過IME/IDM檢查的更改。

1.此圖顯示了IME/IDM上的活動簽名頁籤。

導航到Configuration > Policies > 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 | 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.此圖顯示如何選擇特定的簽名版本。

導航到 Configuration > Policies > Signature Definitions > 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 | Internet 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 Cor... | <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 |

進一步使用filter選項，您可以根據引擎、保真度、嚴重性等過濾特定版本的所有簽名。

通過這樣做，您必須能夠縮小對特徵碼版本所做的更改，這些更改可能是問題發生的潛在原因，您可根據這些原因進行故障排除。