由于SI解析问题，排除FTD阻止专用IP URL故障

目录

问题

当URL主机收到来自Talos的安全情报URL/网络源更新后包含专用IP地址时，FTD设备开始阻止生产内部流量。

受影响的流量包括http://10.54.1.7:8200/v1/sys/health和http://172.31.14.7:9100等URL。流量被分类为“作为主机的私有IP地址”，并被与Talos相关的安全情报策略阻止，判定包括“URL阻止”、“黑名单”和“si， force_block”。 此行为会影响内部服务通信和业务运营。

在检查FTD系统支持跟踪时，观察到以下阻塞行为：

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Firewall: allow rule, 'Access_Rule', allow
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Generating an EOF event with rule_id = 26845
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 SI: URL security intelligence list id 104862
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict: blacklist
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict Reason: si, force_block
```

环境

- 思科FTD版本7.6.4（FMC托管）
- 启用了URL恶意类别的安全情报源
- 在URL中使用私有IP地址的内部生产服务
- 从Talos更新安全情报URL/网络源后出现问题

了解系统支持跟踪日志：

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
```

- 在系统支持跟踪日志中，会打印类别值。
- 类别值：[1048627]
- 类别值和相应的SI源文件的映射在FTD中在以下位置提供：

FTD中的位置：/ngfw/var/sf/siurl_download/url.rules

Tshoot文件中的位置：/file-contents/var/sf/siurl_download/url.rules

<#root>

```
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$

cat url.rules


# security intelligence manifest file
si,5915d129-0d33-4e9c-969a-eab3cde32156.lf,1048589,white,any
si,ac0ef862-1cff-11ef-a575-4cf8bc134a1f.lf,1074790408,block,any
si,005056bf-1643-0ed3-0000-030068648887.lf,1048646,block,any
si,127dc4a2-1ea3-4423-a02d-1f02069828ac.lf,1048590,block,any
si,c87fe5d4-5868-11ef-8843-a8b3afb1bf74.lf,1048645,block,any
si,7c51a74a-d984-11ef-8637-e77eccc0d672.lf,1048649,block,any
si,1b117672-7453-478c-be31-b72e89ca4bfc.lf,1048616,block,any
si,2b15cb6f-a3fc-4e0e-a342-ccc5e5806394.lf,1048619,block,any
si,30f9e69c-d64c-479c-821d-0e4edab852ab.lf,1048620,block,any
si,5f8148f1-e5e4-427a-aa3b-ee1c2745f481.lf,1048623,block,any
si,8af156ca-8020-4608-9278-01b8745811b7.lf,1048626,block,any
si,d3899830-d481-4773-b4e2-7daa7acf8f75.lf,1048633,block,any
si,03709ed4-faab-47af-bade-4435f8da11f5.lf,1048615,block,any
si,bde824fd-36dd-4a7c-9cc1-80e40ac7db66.lf,1048632,block,any
si,a27c6aae-8e52-4174-a81a-47c59fecf1c3.lf,1048629,block,any
si,6ba968f4-7a25-4793-a2c8-7cc77f1f1256.lf,1048625,block,any
si,02213098-6d94-4680-8ce8-2d081638d087.lf,1048613,block,any
si,5a0b6d6b-e2c3-436f-b4a1-48248b333b57.lf,1048622,block,any
si,3e2af68e-5fc8-4b1c-b5bc-b4e7cab5c9eb.lf,1048621,block,any
si,2ccda18e-ddff-4f5c-af9a-f0098521b525.lf,1048618,block,any
si,60f4e2ab-d96c-44a0-bd38-830252b67077.lf,1048624,block,any
si,23f2a124-8278-4c03-8c9d-d28fe08b8fc9.lf,1048617,block,any
si,937cf5e8-76d1-4ba2-a83c-475dc80c6976.lf,1048628,block,any
si,032ba433-c295-11e4-a919-d4ae5275d599.lf,1048614,block,any
si,d7d996a6-6b92-4a56-8f10-e8506e434dd6.lf,1048634,block,any
si,abdc925f-4f85-4504-90a7-c891979af648.lf,1048630,block,any

si,8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf,1048627,block,any >>>>>>matching category ID


si,b1df3aa8-2841-4c88-8e64-bfaacec71300.lf,1048631,block,any
si,ac0f6900-1cff-11ef-a575-4cf8bc134a1f.lf,1074790407,monitor,any
```

```
ac,5846a44a-3d2a-11f0-a12d-7a89a4a10ab3.lf,1048650
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$ pwd
```

如何解释前面的行：

- 名为“8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf”的文件中的内容已分配类别ID:1048627
- 要检查实际的类别，请使用vi和任何编辑器工具打开文件，且类别名称位于顶部。

<#root>

```
kkhapeka@KKHAPEKA-M-F6H2 Downloads %

cat -n  8c3e31be-ca41-43c8-87cb-82a35b0f5213| more


     1  #Cisco DNS and URL intelligence feed: URL Malicious >>>>>name of the category
     2  fadoz.metrs.workers.dev/sell/2641c1ef
     3  oauth-opensea.com
     4  account8133944-complaince.com
```

- 使用逻辑路径可以跟踪相应的安全情报源文件，而收集证据的一个重要方面是将安全情报源文件从FTD手动下载到本地机器。
- 安全情报源会定期更新，在源更新期间，FMC和FTD上不存在指示所做更改的更改日志。
- 通过下载安全情报源，您可以在此刻拍摄源快照，稍后可以将其提供给BU/TALOS。

分辨率

解决方案涉及更新安全情报源，并在等待永久软件修复时实施临时解决方法。

步骤 1：更新安全情报源

更新安全情报源，从Talos获取更正的源内容：

在FMC中导航到Policies > Security Intelligence并手动触发源更新，或等待自动更新周期完成。

步骤 2：实施临时解决方法（如果问题仍然存在）

如果在源更新后问题仍然存在，请将受影响的URL或域添加到“不阻止”列表作为临时解决方法：

导航到Policies > Security Intelligence，并将专用IP URL添加到URL选项卡下的“Do not block”列表。

步骤 3：重新启用URL恶意类别

确认源更新解决问题后，将“URL恶意”类别重新添加到安全情报配置：

导航到Policies > Security Intelligence，并重新启用Block List下的“URL Malicious”类别。

步骤 4：删除解决方法条目

永久修复程序确认且工作正常后，从“不阻止”列表中删除受影响的URL/域。

步骤 5：验证

通过测试以前受影响的URL和监控FMC中的连接事件，验证专用IP URL目标不再被安全情报阻止。

原因

此问题由影响FTD行为的安全情报源内容中的解析问题导致。在安全情报源中，存在长度超过2047个字符的URL。

当条目超过支持的长度时，部分问题可能是因为它错误地加载为单独的恶意条目，从而可能阻止无关的流量。此行为在Cisco Bug ID下跟踪：CSCww11335。此问题通过Talos团队对源内容所做的纠正更改而解决，并计划在后续版本中安装永久软件修复程序，以添加保护轨，防止将来再次发生

。

相关内容

- Cisco Bug ID:CSCww11335
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。