由於SI解析問題導致FTD封鎖私人IP URL疑難排解

目錄

問題

收到來自Talos的安全情報URL/網路源更新後，當URL主機包含專用IP地址時，FTD裝置開始阻止生產內部流量。

受影響的流量包括http://10.54.1.7:8200/v1/sys/health和http://172.31.14.7:9100等URL。流量被分類為「作為主機的私有IP地址」，並被與Talos相關的安全情報策略阻止，其裁決包括「URL阻止」、「黑名單」和「si， force_block」。 此行為會影響內部服務通訊和業務運營。

檢查FTD系統支援追蹤時，會觀察到此封鎖行為：

```
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
```

環境

- Cisco FTD版本7.6.4（FMC代管）
- 啟用了URL惡意類別的安全情報源
- 在URL中使用私有IP地址的內部生產服務
- 來自Talos的安全情報URL/網路源更新後出現問題

瞭解系統支援跟蹤日誌：

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

- 在系統支援跟蹤日誌中，會列印類別值。
- 類別值：[1048627]
- 在FTD中的以下位置提供類別值和對應的SI原始檔的對映：

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

Tshoot檔案中的位置：/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
```

如何解釋前面的行：

- 名為「8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf」的檔案中的內容已分配類別ID:1048627
- 要檢查實際類別是什麼，請使用vi和任何編輯器工具開啟檔案，並且類別名稱位於頂部。

<#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
```

- 使用邏輯路徑可以跟蹤相應的安全情報原始檔，而收集證據的一個重要方面是手動將安全情報原始檔從FTD下載到本地機器。
- 安全情報源會定期更新，在源更新期間，FMC和FTD上不存在指示所做更改的更改日誌。
- 通過下載安全情報源，您可以在此刻拍攝源的快照，稍後可以將其提供給BU/TALOS。

解析

解決方案涉及更新安全情報源，並在等待永久軟體修復時實施臨時解決方法。

步驟 1:更新安全情報源

更新安全情報源，以便從Talos獲取已更正的源內容：

在FMC中導航到Policies > Security Intelligence，然後手動觸發源更新，或等待自動更新週期完成。

步驟 2:實施臨時解決方法（如果問題仍然存在）

如果在源更新後問題仍然存在，請將受影響的URL或域新增到「不阻止」清單中作為臨時解決方法：

導覽至Policies > Security Intelligence，並將私有IP URL新增到URL索引標籤下的「Do not block」清單中。

步驟 3:重新啟用URL惡意類別

確認源更新解決了問題後，將「URL惡意」類別重新新增到安全情報配置中：

導航到Policies > Security Intelligence，並重新啟用Block List下的「URL Malicious」類別。

步驟 4:刪除應對措施條目

永久修復程式確認且工作正常後，從「不阻止」清單中刪除受影響的URL/域。

步驟 5:驗證

通過測試以前受影響的URL並監控FMC中的連線事件，驗證專用IP URL目標不再被安全情報阻止。

原因

此問題是由安全情報源內容中影響FTD行為的分析問題導致的。在安全情報源中，存在長度超過2047個字元的URL。

當條目超出支援的長度時，此問題的部分可能是因為它被錯誤地載入為單獨的惡意條目，從而可能阻止不相關的流量。此行為在思科錯誤ID下追蹤：CSCww11335。此問題通過Talos團隊對源內容進行的更正更改而解決，並計畫在後續版本中安裝永久軟體修復程式，以新增保護軌，防止將來發生。

相關內容

- 思科錯誤 ID:CSCww11335
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。