SI解析の問題によるプライベートIP URLをブロックするFTDのトラブルシューティング

内容

問題

Talosからセキュリティインテリジェンスの URL/ネットワークフィードアップデートを受信した後、URLホストにプライベートIPアドレスが含まれていると、FTDデバイスは実稼働内部トラフィックのブロックを開始しました。

影響を受けるトラフィックには、http://10.54.1.7:8200/v1/sys/healthやhttp://172.31.14.7:9100などのURLが含まれます。トラフィックは「Private IP Addresses as Host」として分類され、「URL Block」、「blacklist」、「si, force_block」などの判定を含むTalos関連のセキュリティインテリジェンスポリシーによってブロックされます。 この動作は、社内のサービスコミュニケーションと業務に影響を与えます。

FTDシステムサポートトレースを調べると、次のブロッキング動作が確認されました。

```
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バージョン7.6.4（FMCマネージド）
- URL Maliciousカテゴリに対応したセキュリティインテリジェンスフィード
- URLでプライベートIPアドレスを使用する内部実稼働サービス

- TalosからSecurity Intelligence URL/ネットワークフィードが更新された後に問題が発生

システムサポートのトレースログについて：

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

- システムサポートのトレースログでは、カテゴリ値が出力されます。
- カテゴリ値： [1048627]
- カテゴリ値と対応するSIフィードファイルのマッピングは、次の場所のFTDで利用できます。

FTD内の場所：/ngfw/var/sf/siurl_download/url.rules

Tshootファイル内の場所：/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
```

上記の行の解釈方法：

- 「8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf」という名前のファイルの内容には、カテゴリID 1048627が割り当てられています。
- 実際のカテゴリを確認するには、 viおよび任意の工ディタツールを使用してファイルを開き、カテゴリの名前が一番上に表示されます。

<#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
```

- セキュリティインテリジェンスフィードファイルに対応する論理パスを使用するとトレースできます。証拠収集の重要な側面の1つは、セキュリティインテリジェンスフィードファイルをFTDからローカルマシンに手動でダウンロードすることです。
- セキュリティインテリジェンスフィードは定期的に更新され、フィードの更新中には、変更内容を示す変更ログがFMCおよびFTDに存在しません。
- Security Intelligenceフィードをダウンロードすると、その時点でのフィードのスナップショットを取得でき、後でBU/TALOSに提供できます。

解決方法

この問題の解決には、セキュリティインテリジェンスフィードの更新、およびソフトウェアの修正が恒久的に行われるまで一時的な回避策の実施が含まれます。

手順1：セキュリティインテリジェンスフィードの更新

Security Intelligenceフィードを更新して、Talosから修正されたフィードコンテンツを取得します。

FMCでPolicies > Security Intelligenceに移動し、フィードの更新を手動でトリガーするか、自動更新サイクルが完了するのを待ちます。

ステップ2：一時的な回避策の実装（問題が解決しない場合）

フィードの更新後も問題が解決しない場合は、一時的な回避策として、影響を受けるURLまたはドメインを「ブロックしない」リストに追加します。

Policies > Security Intelligenceの順に移動し、プライベートIP URLをURLタブの下の「Do not block」リストに追加します。

ステップ3:URLの悪意のあるカテゴリを再度有効にする

フィードアップデートで問題が解決したことを確認したら、Security Intelligenceの設定に「URL Malicious」カテゴリを再度追加します。

Policies > Security Intelligenceの順に移動し、Block Listの下の「URL Malicious」カテゴリを再度有効にします。

ステップ4：回避策のエントリを削除する

恒久的な修正が確認され、動作したら、「ブロックしない」リストから影響を受けるURL/ドメインを削除します。

ステップ5：検証

以前に影響を受けたURLをテストし、FMCで接続イベントをモニタリングして、プライベートIP URLの宛先がSecurity Intelligenceによってブロックされていないことを確認します。

原因

この問題は、FTDの動作に影響を与えるセキュリティインテリジェンスフィードのコンテンツの解析に関する問題が原因で発生しました。セキュリティインテリジェンスフィードに、長さが2047文字を超えるURLがありました。

エントリがサポートされている長さを超える場合、この問題の一部として、別の悪意のあるエントリとして誤ってロードされ、無関係なトラフィックをブロックしたことが考えられます。この動作は、Cisco Bug ID CSCww11335で追跡されています。この問題は、Talosチームによってフィードコンテンツに対して行われた修正の変更によって解決され、今後のリリースでガードレールを追加して将来の発生を防止するための恒久的なソフトウェア修正が計画されています。

関連コンテンツ

- Cisco Bug ID:CSCww11335
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。