7.4.3から7.6.4へのアップグレード後のFTD管理インターフェイスの障害

内容

問題

Cisco Secure Firewall 3130 Threat Defense(FTD)High Availability(HA)ペアをバージョン7.4.3から7.6.4にアップグレードした後、Firewall Management Center(FMC)でプライマリユニットに障害が99 %完了して応答しなくなった。セカンダリユニットが正常にアップグレードされ、HAペアでアクティブになりました。プライマリユニットがSSH接続に応答せず、FMCがプライマリユニットと通信できませんでした。

調査の結果、FXOSで次の重大な障害が確認されました。

```
Critical  F1000398 2026-08-14T20:52:06.297     58437 [FSM:FAILED]: out-of-band interface configuration(
```

FTDアップグレードログには、アップグレードが実際に正常に完了（100 %完了）したことが示されましたが、SFTunnelサービスが正しく開始されず、FTDとFMC間の通信が妨げられています。デバイスは、自身、ゲートウェイ、およびピアFTDユニットにpingを実行できましたが、異なるサブネットに存在するFMCには到達できませんでした。

環境

- Cisco Secure Firewall 3130 Threat Defense HAペア
- 元のソフトウェアバージョン：FTD 7.4.3
- ターゲットソフトウェアバージョン：FTD 7.6.4（ビルド69）
- Cisco Firepower Extensible Operating System(FX-OS)v2.16.1（ビルド147）
- 静的IPアドレッシングで設定された管理インターフェイス

- FTD管理ネットワークとは異なるサブネットにあるFMCサーバ

解決方法

この問題は、該当のFTDユニットで管理インターフェイスを完全に再設定することで解決されました。次の手順が実行されました。

ステップ1:SSHが機能していなかったため、コンソールアクセスを使用してFTDに接続します。

ステップ2：アップグレードログをチェックして、アップグレード完了ステータスを確認します。

```
root@device:/ngfw/var/log/sf/Cisco_FTD_SSP_FP3K_Upgrade-7.6.4# cat status.log
```

ステップ3:FXOSの管理インターフェイスの障害を確認します。

```
device# show fault
```

ステップ4：管理IPアドレスを再設定して、基本的なトラブルシューティングを試みます（これで問題は解決しませんでした）。

ステップ5：コールドリブートを実行します（これで問題は解決しませんでした）。

ステップ6:FTD CLIからmanagement0インターフェイスを完全に無効にします。

```
configure network management-interface disable management0
```

ステップ7:management0インターフェイスを再びイネーブルにします。

```
configure network management-interface enable management0
```

ステップ8：管理インターフェイスのネットワーク設定を再設定します。

```
configure network ipv4 manual <ip_address> <netmask> <gateway>
```

ステップ9:FXOSアラートがクリアされ、FTDがFMCにpingできるようになったことを確認します。

```
root@device:/# ping <FMC_IP_address>
```

ステップ10:manage_procs.plスクリプトを使用して、SFTunnelサービスを再起動します。

```
manage_procs.pl restart sftunnel
```

ステップ11:SFTunnel接続を確認します。

```
root@device:/# sftunnel_status.pl
```

ステップ12：フェールオーバー機能をテストして、HA操作が正しく動作していることを確認します。

これらの手順が完了すると、FTDはFMCと正常に通信できるようになり、すべての接続テストとフェールオーバーテストが成功しました。ホットフィックスアップグレードは、問題なく適用できます。

原因

根本的な原因は、アップグレードプロセスが正常に完了しているにもかかわらず、7.4.3から7.6.4へのFTDのアップグレード後に、管理インターフェイスが正しく初期化されないことにあります。アップグレードプロセス中にアウトオブバンド管理インターフェイス設定(OMI)有限状態マシン(FSM)に障害が発生し、管理インターフェイスが適切な接続を確立できませんでした。この動作は、Cisco Bug ID CSCww08417に記載されています。

この問題は、以前に報告された不具合のCisco Bug ID CSCwj04154およびCisco Bug ID CSCwa69303に似ていますが、異なる状況で発生します。管理インターフェイスで障害が発生し

たため、アップグレードが99 %完了したと誤った印象が表示されました。実際には、アップグレードは正常に完了しましたが、管理接続が切断されています。

関連コンテンツ

- Cisco Bug ID CSCww08417：アップグレード後、FTD管理インターフェイスが起動しないことがある
- Cisco Secure Firewall Threat Defense 互換性ガイド
- 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。