アップグレード障害の影響を受ける17.12上のCatalyst APの検証と回復

内容

はじめに

このドキュメントでは、Cisco Bug ID CSCwf25731 およびCSCwf37271

影響を受けるアクセスポイント

次のアクセスポイントモデルは影響を受けます。以下のモデルを使用していない場合は影響を受けず、それ以上の操作は必要ありません。

- Catalyst 9124(I/D/E)
- Catalyst 9130(I/E)
- Catalyst 9136I
- Catalyst 9162I
- Catalyst 9163E
- Catalyst 9164I
- Catalyst 9166(I/D1)

- Catalyst IW9167(I/E)

CONTEXT

17.12.4/5/6aにあるシステムから任意のリリースにアップグレードすると、特定の条件下で特定のアクセスポイントモデルがブートループに入る可能性があります。これは、ターゲットデバイスのストレージ上のディスク領域が不足しているためにイメージのインストールが失敗したことが原因です。このシナリオは、ISSU、フルコントローライメージのインストール、APSPなど、アクセスポイントに関連するアップグレード操作中にのみ発生し、通常のサービス、日常的な操作、またはSMUのインストールには影響しません。

影響を受ける可能性のあるアクセスポイントでアップグレードを実行する前に、追加の手順を実行する必要があります。この問題には回避策がなく、設定、導入タイプ、コントローラモデルに依存しません

この問題は、17.12.4より前のバージョンには影響しません。また、アクセスポイントで17.12.6aより後のリリース（17.15.xなど）が実行されており、影響を受けるバージョンがインストールされていない場合も影響を受けません。

Cisco IOS XEリリース17.12.4、17.12.5、17.12.6aについては、それぞれのAPSPの形式で修正が利用可能です。また、影響を受けるリリースを使用していて、すでに新しいバージョンにアップグレードされている導入の場合、17.15.4dと17.18.2で失われたスペースを回復するために、クリーンアップAPSPを使用できます。

いずれかの時点でネットワークが該当リリースにアップグレードされている場合、またはネットワークがそれらのバージョンを以前に使用したことがあるかどうかわからない場合は、予防策として、アップグレードの前にチェックを実行することを推奨します

根本原因の詳細

コード17.12.4 ~ 17.12.6aを実行する該当モデルのアクセスポイントでは、永続的なファイル「/storage/cnssdaemon.log」を作成します。このファイルは1日あたり5 MBまで拡張でき、そのディスクパーティション上の使用可能な領域をすべて使用できます。このファイルは再起動時にクリアされません。 パーティションが完全に使用されると、新しいファイルバージョンを保存するための重要な手順が完了しないため、アップグレードが失敗する可能性があります。

この問題は、内部コンポーネントのログの宛先を変更したライブラリの更新によって発生しました。デバイスの操作にログファイルは必要ありません

アップグレード障害が発生するのは、APがパーティション1から実行されており、パーティション2のスペースが使い果たされている場合だけです。十分な空き容量がある場合、またはAPがパーティション2から起動した場合、アップグレードは成功します

アップグレードチェック手順

WLCが現在17.12.4、17.12.5、17.12.6a上にある場合は、次の手順を実行する際に、修正を含む

ソフトウェアバージョンへのアップグレードが必須になります。 WLCにインストールされている他のバージョンで、アップグレードを計画している場合、次の手順に従うことを強く推奨します。

ステップ1：アクセスポイントが影響を受ける可能性があるかどうかを確認します（表1を参照）。 影響を受けない場合は、事前チェック/リカバリプロセスは不要です。最新リリースへのアップグレードに直接進むことができます。

ステップ2：影響を受ける場合は、プレチェックを実行して、プレチェックセクションで影響を受けるAPの数を識別します。

ステップ3：特定したAPで、「リカバリ」セクションに記載されているリカバリ手順を実行します。

ステップ4：事前チェックを再実行して、他のAPが影響を受けていないことを確認します。

ステップ5：修正済みバージョンの表に記載されている各APSPまたはソフトウェアバージョンへのアップグレードに進みます。

この通知がご自分に当てはまるかどうかを確認するには、次の表を参照してください。

表1：アップグレードパスの適用性

現在のバージョン	target	問題の適用性	アップグレード前に事前チェックが必要	ターゲット/アップグレードパス	アップグレードの事前チェック	注釈
17.3.x / 17.6.x / 17.9 x	17.12.x	いいえ	いいえ	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	いいえ	インストール先のリリースノートを確認
17.9.x	任意 (17.12.4/5/6aを除く)	いいえ	いいえ	アップグレード先のパスに従う	いいえ	17.9.1から。5への直接アップグレードはサポートされてい

						ません。 17.9.6以降を使用してください。 詳細については、リリースノートを参照してください。
17.12.1 ~ 17.12.3	任意 (17.12.4/5/6a以外)	いいえ	いいえ	アップグレード先のパスに従う	通常のプロセス	インストール先のリリースノートを確認
17.12.4/5/6a	17.12.x（4、5、6aなど）、APSP	Yes	Yes	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	Yes	修正済みのAPSPをインストールした後は、将来の17.12アップグレードのために追加の事前確認は必要ありません
17.12.4/5/6a	17.15.x / 17.18.x	Yes	Yes	それぞれの17.12.x APSPをアップグレードしてから、17.15.x + APSPxまたは17.18.x + APSPxにアップグレード	最初の17.12 APSPアップグレードでは「はい」で、それ以降のアップグレードでは「いいえ」です。	
どのリリースでも、以前のイメージは17.12.4/5/6aのいずれかでした。	17.15.x	Yes	Yes	17.15.x + APSPx	Yes	
どのリリースでも、以前のイメージは17.12.4/5/6aのいずれかでした。	17.18.x	Yes	Yes	17.18.x + APSPx	Yes	

17.15+ 新規導入	[Any]	いいえ	いいえ	[Any]	いいえ	
17.18. 新規導入	[Any]	いいえ	いいえ	[Any]	いいえ	

注：一般に、ネットワークが稼働しておらず、過去に17.12.4、17.12.5、17.12.6aが稼働していない場合、この問題は該当しません

注：「現在」の列に明示的に記載されていない他のリリースは、推奨アップグレードパスに従います。

修正済みリリース

コントローラ	APイメージバージョン
17.12.4 + APSP13	17.12.4.213
17.12.5 + APSP9	17.12.5.209
17.12.6a + APSP1	17.12.6.201
17.15.3 + APSP12	17.15.3.212
17.15.4b + APSP6	17.15.4.206
17.15.4d + APSP1	17.15.4.225
17.18.1 + APSP3	17.18.1.203
17.18.2 + APSP1	17.18.2.201

事前チェック

ネットワークがこの問題の影響を受けやすいかどうかを確認するには、現在の手順に従います。これらの手順は概要を説明するのに役立ちますが、APの実際の検出については、「プレチェック

スクリプト」の項を使用してこのプロセスを自動化してください。

- 影響を受けるリリースの場合は、プライマリイメージ列またはバックアップイメージ列でアクセスポイントイメージが一致しているかどうかを確認します。

```
9800-l#show ap image
Total number of APs  : 4

Number of APs
        Initiated                 : 0
        Downloading               : 0
        Predownloading            : 0
        Completed downloading     : 0
        Completed predownloading  : 0
        Not Supported             : 0
        Failed to Predownload     : 0
        Predownload in progress   : No

AP Name             Primary Image          Backup Image            Predownload Status   Predownload Ver
-------------------------------------------------------------------------------------------------------
Ap1                 17.12.5.41        17.12.4.201               None                 0.0.0.0
Ap2                 17.12.5.41        17.12.4.201               None                 0.0.0.0
Ap3                 17.12.5.41        17.12.4.201               None                 0.0.0.0
Ap4                 17.12.5.41        17.12.4.201               None                 0.0.0.0
```

- APでも同様の検証を実行できます。

```
AP# show version
AP Running Image     : 17.12.5.41
Primary Boot Image   : 17.12.5.41
Backup Boot Image    : 17.12.5.209
Primary Boot Image Hash: 93ef1e703a5e7c5a4f97b8f59b220f52d94dd17c527868582c0048caad6397a9f3526c644f94a5
Backup Boot Image Hash: 4bbe4a0d9edc3cad938a7de399d3c2e08634643a2623bae65973ef00deb154b8eb7c7917eeecdd4
1 Multigigabit Ethernet interfaces

Any Boot Image is one of the following:
- 17.12.4.0 to 17.12.4.212
- 17.12.5.0 to 17.12.5.208
- 17.12.6.0 to 17.12.6.200
```

- 現在のブートパーティションを確認します。

```
AP# show boot
--- Boot Variable Table ---
BOOT path-list: part1
Console Baudrate: 9600 Enable Break:

The “BOOT path-list:” should be part1, suggesting that the Backup partition is running on part2.
```

- 現在のファイルシステムの使用状況を確認します。

```
AP# show filesystems
Filesystem                Size      Used Available Use% Mounted on
devtmpfs                880.9M         0    880.9M   0% /dev
/sysroot                883.8M    219.6M    664.1M  25% /
tmpfs                     1.0M     56.0K    968.0K   5% /dev/shm
tmpfs                   883.8M         0    883.8M   0% /run
tmpfs                   883.8M         0    883.8M   0% /sys/fs/cgroup
/dev/ubivol/part1       372.1M     79.7M    292.4M  21% /part1
/dev/ubivol/part2       520.1M    291.3M    228.9M  56% /part2

The “Use%” for “/dev/ubivol/part2” is close to 100%.
```

- 両方のパーティションのイメージの整合性を確認します。

```
AP# show image integrity
/part1(Backup) 17.12.5.209
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good
/part2(primary) 17.12.5.41
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good

The image integrity should be “Good” for all fields in both the partitions. If not Good open a TAC case
```

次のセクションでは、すべてのAPのプレチェックプロセスを自動化するスクリプトについて説明します。

事前確認スクリプト

WLANポーラー(こちらからダウンロードできます)

ステップ1:WLANポーラーを目的のファイルの場所に抽出します

ステップ2:「config.ini」ファイルの次の値を変更します。

```
wlc_type: 2
mode: ssh
ap_mode: ssh

; set global WLC credentials
wlc_user: username
wlc_pasw: password
wlc_enable: enable_password
```

```
; set global AP credentials
ap_user: ap_username
ap_pasw: ap_password
ap_enable: ap_enable_password

[WLC-1]
active: True
ipaddr:


mode: ssh
```

ステップ3:残りのデフォルトの内容と下記のコマンドリストを、「cmdlist_cos」および「cmdlist_cos_qca」ファイルにコメント化します。

```
show clock
show version
show flash
show flash | i cnssdaemon.log
show boot
show filesystems
show image integrity
```

次に例を示します。

```
# snippet to download the Debug image on COS APs
# show version | in Compiled
# archive download-sw /reload tftp://


        /


#
show clock
show version
show flash
show flash | i cnssdaemon.log
show boot
show filesystems
show image integrity
```

ステップ4:「。\wlanpoller.exe」を使用してwlanpollerを実行します。WLANポーラーが実行され、すべてのAPにSSHで接続され、それらすべてのAPに対するこれらのコマンドの出力が取得さ

れます。

ステップ5：実行後、「data」フォルダが作成されます。フォルダを入力し、各AP用に複数のファイルを作成した最後まで移動します。

ステップ6:このフォルダに個別に提供された「ap_detection_script.py」をコピー/ペーストして実行します。スクリプトは、次のボックスのリンクにあります。

https://pubhub.devnetcloud.com/media/wireless-troubleshooting-tools/docs/9800-scripts/ap_detection_script.zip

これにより、同じフォルダに「Status_check_results.log」という名前でファイルが作成されます。このリストには、問題が発生する可能性のあるAPのリストが含まれており、アップグレードを開始する前に回復や追加の手順が必要になります。

リカバリプロセス：

問題があると判断された各アクセスポイントの現在の状態に基づいて、これらのAPを回復するために最も最適化される方法に関するガイダンスを提供します。 各オプションで実行する必要がある詳細な手順を次に示します。

オプション1：パーティションスワップ

ステップ1:APが以前のパーティションまたはバージョンに戻らないようにするために、APがコントローラと通信できないことを確認します。これは、コントローラゲートウェイ上のアクセスリストによって実現できます。

ステップ2：影響を受ける可能性のあるAPから、パーティション2のブートを設定します。

```
AP# config boot path 2
```

ステップ3:APをリブートして、パーティション2のイメージでAPが起動するようにします。

```
AP# reset
```

ステップ4：コントローラのアップグレードが完了した後に、APをコントローラに加入させます。APが加入し、新しいイメージをダウンロードします。

注：このオプションが何らかの理由で実行できない場合は、いつでもTACケースをオープンし、このAPセットに対してもオプション2に進むことができます。

オプション2:TACケースを開いて、TACがルートシェルからAPをクリーンアップす

るようにする（このプロセスの後で、通常のアップグレードを行います）

オプション3：安全な状態だが、バックアップパーティションのAPのイメージがバグしている

APは、ほとんどの場合、修正済みバージョンへのアップグレードが完了した後、この状態になります。この状態は、APが修正済みバージョンを実行しているが、バックアップバージョンはまだバグがあることを示しています。注意が必要な場合は、APのバックアップを適切なイメージ（この問題が発生しないバージョン）に置き換えることをお勧めします。対象のAPの数に応じて、APにイメージをアーカイブしてダウンロードするか、または実際にアクティブ化せずに事前ダウンロードを実行します。

オプション4：これらのAPのイメージ整合性チェックが失敗した

アップグレードを進める前に、TACのサービスリクエストをオープンし、TACエンジニアにこれらのAPを修正してもらいます。

オプション5：これらのAPのイメージ整合性チェックが失敗した

現在のパーティションは影響を受けませんが、フラッシュストレージが少なくなっています。TACを開き、ストレージからdevshellを介してcnssdaemon.logをクリーンアップすることをお勧めします。

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。