2022年12月4日の期限切れイメージ署名証明書のポストが原因で失敗するIOS APイメージのダウンロード(CSCwd80290)

内容

概要

このドキュメントでは、2022年12月4日以降に、AireOSとC9800 Wireless LAN Controller(WLC)の両方で発生するIOSアクセスポイント(AP)の加入の障害について詳しく説明します。この問題は、Cisco Bug CSCwd80290およびField NoticeFN72524で追跡されており、APイメージ署名証明書の検証のの障害がが原因です。

該当製品

802.11ac Wave 1 AP（IW3702/3700/2700/1700/1570シリーズ）および700/1530/1550/3600/2600/1600/3500/AP8を含む以前のAPが該当します。 02/AP803シリーズ。該当するLightweight IOSイメージは、2012年12月から2022年11月にかけて作成されたものです。AireOS、Catalyst 9800シリーズ、およびコンバージドアクセスコントローラが該当します。AP-COSが稼働するAP(802.11ac Wave 2、Wi-Fi 6、Wi-Fi 6E AP)は影響を受けず、AutonomousモードのIOS APも影響を受けません。

問題

2022年12月4日以降にCAPWAPを使用してIOS APをアップグレードまたはダウングレードすると、イメージのダウンロードループに陥り、ダウンロードされたイメージ内の署名証明書の検証に失敗するためにWLCへの加入が失敗する場合があります。

根本原因

AP IOSイメージにバンドルされているイメージ署名証明書は、2012年12月4日に発行され、2022年12月4日に期限切れになりました。IOS APは、APにソフトウェアをインストールする前に、この証明書を使用してWLCからダウンロードしたイメージを検証します。そのため、2022年12月4日以降、ソフトウェアのアップグレード/ダウングレードや、異なるバージョンを実行するWLC間での移動が原因でAPがコードをダウンロードすると、APはイメージの検証に失敗し、ダウンロードのイメージループに無期限に留まります。この問題は、すべてのAireOSおよびIOS-XEバージョンで発生します。

症状

この問題が発生しているかどうかを確認するには、まずWLCでAPがDownloadingステータスのままになっていないかどうかをチェックします。 次に、問題を確実に特定するために、ssh、telnet、またはコンソールを使用して影響を受けるAPに接続し、それらの口グを表示します（または、syslogサーバでAP口グを探します）。

AireOS WLC上

WLCで、show ap image status(AireOS 8.10)を実行すると、影響を受けるAPが「Downloading」ステータスで表示されます。

8.5では、show ap image allを使用すると、「Downloading」にゼロ以外の数のAPが表示されます。

```
(AireOS WLC-8.5) >show ap image all

Total number of APs.............................. 1
Number of APs
        Initiated....................................... 0
        Downloading..................................... 1
        Predownloading.................................. 0
        Completed predownloading........................ 0
        Not Supported................................... 0
        Failed to Predownload........................... 0

                                                 Predownload     Predownload
AP Name            Primary Image  Backup Image   Status          Version         Next Retry Time  Retry
------------------ -------------- -------------- --------------- --------------- ---------------- ------
AP1700             8.5.182.0      0.0.0.0        None            None            NA               NA

(AireOS WLC-8.10) >show ap image status
Total number of APs.............................. X
Total AP's Downloading........................... 1
AP Name            Primary Image  Download Status
------------------ -------------- ---------------
```

```
CAP3702E.4CD4      17.3.6.76      Downloading
```

IOS-XE C9800 WLCの場合

C9800#show ap summary

```
9800-L#show ap summary

AP Name                           Slots    AP Model  Ethernet MAC    Radio MAC       Location
-----------------------------------------------------------------------------------------------
AP2702E                             2      2702E     0081.c4fb.2e74  843d.c673.10d0  default location
```

この問題が発生すると、APログに次のようなエラーが表示されます。

SHA-1 AP（2014年中頃に製造）:

```
*Dec 6 21:35:24.259: Using SHA-1 signed certificate for image signing validation.
*Dec 6 21:35:24.327: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The c
*Dec 6 21:35:24.327: Image signing certificate validation failed (1A).
*Dec 6 21:35:24.327: Failed to validate signature
*Dec 6 21:35:24.327: Digital Signature Failed Validation (flash:/update/ap3g2-k9w8-mx.153-3.JPJ9/final_
*Dec 6 21:35:24.327: AP image integrity check FAILED
```

SHA-2 AP（2014年中頃に製造）:

```
*Dec 6 08:47:20.159: Using SHA-2 signed certificate for image signing validation.
*Dec 6 08:47:20.223: DTLS_CLIENT_ERROR: ../capwap/base_capwap/dtls/base_capwap_dtls_record.c:169 Pkt to
*Dec 6 08:47:20.227: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The c
*Dec 6 08:47:20.227: Image signing certificate validation failed (1A).
*Dec 6 08:47:20.231: Failed to validate signature
*Dec 6 08:47:20.231: Digital Signature Failed Validation (flash:/update/ap3g2-k9w8-mx.153-3.JPJ7c/final
*Dec 6 08:47:20.231: AP image integrity check FAILED
```

回避策

修正済みソフトウェアを実行していない場合は、次の手順に従ってIOS APの加入を許可します。

1. NTPを無効にして、コントローラが自動的に時刻転送を設定しないようにします。

```
AireOS:
```

```
(AireOS WLC)>show time

make a note of all configured NTP servers, and delete each one:

(AireOS WLC)>config time ntp delete
```

```
      IOS-XE: C9800#show run | i ntp ntp server ip
```

```
       C9800#config terminal (config)#no ntp server ip
```

```
        ! for each configured NTP server
```

2. WLCの日付を、2022年12月4日（2022年11月1日）より前の日付に変更します。これは、コントローラまたは新しいAPで証明書が無効になる可能性があるためです。

```
(AireOS WLC)> config time manual 12/02/22 00:00:00

C9800#clock set 00:00:00 2 Dec 2022
```

3. WLCの時刻が変更されたことを確認します

```
(AireOS WLC)> show time
Time..................................... Fri Dec  2 00:00:02 2022

C9800#show clock
00:00:02.573
```

```
Fri Dec 2 2022
```

4.すべてのAPが新しいイメージでRegistered状態になるまで待ちます。

> 注：場合によっては、日付の変更後にAPを加入させるためにAPのリブートが必要になることがあります。ただし、APをリブートする前に、APが再度加入できるようになるまで少なくとも30分待ってください

5. NTPを再度有効にします。

```
(AireOS WLC)>config time ntp server 1
```

```
C9800#configure terminal (config)#ntp server ip
```

6.設定を保存します。

```
(AireOS WLC)>save config
Are you sure you want to save? (y/n) y

C9800#write memory
```

7. WLCのクロックの再確認

```
(AireOS WLC)>show time
C9800# show clock
```

修正済みソフトウェアへのアップグレード

AireOS WLC上

1. ダウンロード中にAPがスタックする場合は、ソフトウェアにアップグレードする前にAPがダウンロードを完了してRegistered状態で起動できるように、コントローラのタイムバックを設定します。
    1. タイムバックの設定の詳細については、上記の「回避策」のセクションを参照してください

    2. 運用上の理由でタイムバックを設定できない場合は、スイッチポートをシャットダウンしたり、CAPWAPをブロックするACLをインストールするなどして、該当するIOS APがコントローラへの加入を試行するのをブロックします。

2. APがDownloading状態になっていないため、WLCの時刻が現在の時刻に設定されていることを確認します（NTPを再度有効にします）。
3. 修正済みソフトウェアをAireOS WLCにインストールします（8.10.183.0以降。8.5からアップグレードできない場合は、8.5メインラインを使用している場合は8.5.182.7を、8.5 IRCMの場合は8.5.182.105を使用します）。修正済みソフトウェアをダウンロードするには、次のリンクを参照してください。
    - 8.10

8540:https://software.cisco.com/download/home/286284728/type/280926587/release/8.10.183.0

5520:https://software.cisco.com/download/home/286284738/type/280926587/release/8.10.183.0

3504:https://software.cisco.com/download/home/286312601/type/280926587/release/8.10.183.0

vWLC:https://software.cisco.com/download/home/284464214/type/280926587/release/8.10.183.0

- 8.5（隠し投稿）

8.5.182.7（8.5メインライン）:https://software.cisco.com/download/specialrelease/8f166c6d88b9f77aabb63f78affa9749。

8.5.182.105(8.5 IRCM):https://software.cisco.com/download/specialrelease/bc334964055fbd9440834f008e5aca34。

4. （任意）リブートする前に、加入したAPに修正済みソフトウェアをプレダウンロードします。
5. WLC のリブート.
6. APスイッチポートまたはブロックされたCAPWAPをシャットダウンする場合は、ブロックを削除して、IOS APが再加入してアップグレードできるようにしますを参照。

IOS-XE 9800 WLCの場合

1. 17.3.6、17.6.4、17.9.2 IOS-XEソフトウェアを9800フラッシュにダウンロードします。ご使用の環境のAPモデルと使用中の機能に基づいて環境に最適なバージョンを選択するには、『C9800 WLC向けの推奨IOS XEリリース』を参照してください。

2. 17.3.6 APSP7または17.6.4 APSP1または17.9.2 APSP1ファイル（IOS AP修正済み）を9800フラッシュにダウンロードします。

- 17.3.6:17.3.6 APSP7(CSCwd83653/CSCwe10047を使用)（修正プログラムはAPSP2およびAPSP5にも含まれる）

9800-40:https://software.cisco.com/download/home/286316412/type/286325254/release/17.3.6

9800-80:https://software.cisco.com/download/home/286321396/type/286325254/release/17.3.6

9800-CL:https://software.cisco.com/download/home/286322605/type/286325254/release/17.3.6

9800-L:https://software.cisco.com/download/home/286323430/type/286325254/release/17.3.6

- 17.6.4:17.6.4 APSP1（IW3702用）、CSCwd87305経由

9800-40:https://software.cisco.com/download/home/286316412/type/286325254/release/17.6.4

9800-80:https://software.cisco.com/download/home/286321396/type/286325254/release/17.6.4

9800-CL:https://software.cisco.com/download/home/286322605/type/286325254/release/17.6.4

9800-L: https://software.cisco.com/download/home/286323430/type/286325254/release/17.6.4

- 17.9.2:17.9.2 APSP1（IW3702向け）経由CSCwd87612

9800-40:https://software.cisco.com/download/home/286322605/type/286325254/release/17.9.2

9800-80:https://software.cisco.com/download/home/286321396/type/286325254/release/17.9.2

9800-CL:https://software.cisco.com/download/home/286322605/type/286325254/release/17.9.2

9800-L:https://software.cisco.com/download/home/286323430/type/286325254/release/17.9.2

注：
1) 17.3.6 APSP7 には、CSCwd80290 に加え、複数のバグ (CSCvx32806、CSCwc32182、CSCvz99036、CSCwd37092、CSCwc78435、CSCwc88148) に対する修正が含まれています。
2) 17.6.4 APSP1 には、CSCwd80290（IW3700用）に加え、複数のバグ (CSCwc73090、CSCwc71198、CSCwc78435、CSCwd40731、CSCvx32806) に対する修正が含まれています。

---

3. 17.3.6がすでにインストールされていない場合は、17.3.6 IOS-XEを今すぐインストールしてリ

ロードします。

```
C9800#install add file bootflash:/C9800-L-universalk9_wlc.17.03.06.SPA.bin activate commit
```

4. 9800がリブートした後 – コントローラの時刻が時間に戻っていた場合は、現在の時刻に設定します（NTPを再度有効にします）。

5 APSP7をインストールしてIOS APを回復します。

```
C9800#install add file bootflash:/C9800-universalk9_wlc.17.03.06.CSCwe10047 .SPA.apsp.bin
C9800#install activate file bootflash:/C9800-universalk9_wlc.17.03.06.CSCwe10047 .SPA.apsp.bin
C9800#install commit
```

よく寄せられる質問（FAQ）

- この問題が原因で、現在登録されているAPが接続解除されるか、または接続に失敗しますか。
  WLCと同じバージョンを実行しているAPは、問題なく動作し続け、正常にブートして接続します。この問題は、イメージアップグレードの一部として行われるイメージ検証プロセスにのみ影響します。

- APのプレダウンロードは影響を受けますか。

はい。APのプレダウンロードには、APへのイメージのダウンロードとAPによるイメージの検証が含まれるため、同じ期限切れ証明書とイメージ検証エラーが発生します。

- 時間の変更によってサービスにどのような影響がありますか。お客様は、これを正午に実行できますか。それとも、ダウンタイムとサービスへの影響を伴うメンテナンス期間をスケジュールする必要がありますか。
  コントローラの時刻を変更しても、APの加入やワイヤレスクライアントの接続に運用上の影響はありません。ただし、DNA Center Assurance、CMX、およびCisco(DNA)Spacesが影響を受ける可能性があります。APが加入し、時刻が現在の時刻に戻ると、これらのサービスは回復すると予想されます。

- 実稼働コントローラで時刻を設定できない場合はどうすればいいですか。
  実稼働WLCと同じコードバージョンでステージングWLCを設定します（vWLCまたは9800-CLも動作します）。ステージングWLCで時刻を元に戻し、APをステージングWLCに参加させます。APがコードをダウンロードし、ステージングWLCで登録済み状態に移行したら、APを実稼働WLCに移動します。

- 修正済みバージョンのインストール時間を変更する必要がありますか。

AireOSでのみ、APがdownloading状態のままになっている場合詳細については、「修正済みソ

フトウェアへのアップグレード」の項を参照してください。

- 新しいAPを追加するとどうなりますか。
  新しいAPがコントローラと同じバージョンでインストールされている場合、APは問題なく加入します。
  一方、バージョンが一致しない場合、APは対応するイメージをダウンロードしようとします。コントローラ上のコードに修正済みのAPバンドルイメージがない場合、これによりAPは前述のようにアップグレードに失敗し、回避策が必要になります。
  コントローラが修正済みバージョンのいずれかにアップグレードされている場合は、新しいAPを通常どおり追加して、アップグレードプロセスを完了できます。

- RMAから受け取ったユニットはどうなりますか。
  これは、新しいAPを追加することと同じです。APイメージの修正を含むコントローラバージョンを実行している場合は、通常どおり加入してアップグレードします。
  それ以外の場合は、時間回避策を適用します。

- 運用のために時間を変更しておく必要がありますか。
  いいえ、APのアップグレードプロセスが完了したら、コントローラを現在の時刻に戻し、NTPを再度有効にできます。

- APログに「%PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Certificate chain validation has failed.」というエラーが表示されます。証明書(SN: xx)はまだ有効ではありません。有効期間は2022年3月1日のHH:MM:SS UTCから始まります。これは同じ症状ですか、それとも新しい症状ですか。

このエラーは、WLCのクロックが、証明書（この場合）の開始日である2022年3月1日よりも後ろに設定されていることを示しています。この日付は、WLCが製造された時期、または仮想WLC上の自己署名証明書が生成された時期によって異なります。

WLCのクロックを変更して、証明書を有効にします。

- この問題の再発を防ぐために、シスコは何を行っていますか。
  すべてのエンタープライズ製品について完全な監査を実施し、検出されなかった可能性がある同様の問題を特定して、是正措置を実施します
  また、この問題を修正するために、IOS APイメージバンドルプロセスに変更が適用されています。

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。