2022年12月4日之後到期的映像簽名證書導致IOS AP映像下載失敗(CSCwd80290)

目錄

簡介

本檔案提供有關IOS存取點(AP)加入失敗的詳細資訊，請參閱AireOS和C9800無線LAN控制器(WLC)在2022年12月4日之後發生的故障。此問題由Cisco錯誤CSCwd80290和現場通知FN72524追蹤並由AP映像簽署憑證驗證失敗所導致。

受影響的產品

此問題影響執行IOS的所有輕量型存取點 — 包括：802.11ac Wave 1 AP（IW3702/3700/2700/1700/1570系列）和早期的AP(包括700/1530/1550/3600/2600/3500/AP802/AP8 03系列。受影響的輕量IOS映像的構建時間為2012年12月至2022年11月。AireOS、Catalyst 9800系列和融合接入控制器受到影響。 運行AP-COS(802.11ac Wave 2、Wi-Fi 6、Wi-Fi 6E AP)的AP不受影響，IOS AP也不處於自主模式。

問題

當通過CAPWAP升級或降級IOS AP時，在2022年12月4日之後，它們可能會停滯在映像下載環路中，從而無法加入WLC，因為無法驗證下載映像中的簽名證書。

根本原因

捆綁在AP IOS映像中的映像簽名證書於2012年12月4日頒發，並於2022年12月4日到期。在AP上安裝軟體之前，IOS AP使用此憑證驗證從WLC下載的映像。因此，在2022年12月4日之後，當AP由於軟體升級/降級或在運行不同版本的WLC之間移動而下載代碼時，AP將無法驗證映像並將無限期地保持在下載映像循環中。所有AireOS和IOS-XE版本均出現問題。

症狀

要驗證您是否遇到此問題，首先在WLC上檢查是否有AP停滯在「下載」狀態。 然後，為了正確識別問題，請通過ssh、telnet或控制檯訪問受影響的AP並檢視其日誌（或者在syslog伺服器上查詢AP日誌）。

在AireOS WLC上

在WLC上，show ap image status(AireOS 8.10)將受影響AP顯示為「下載」狀態。

在8.5中，使用show ap image all，此影象將在「下載」中顯示非零數量的AP。

```
(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
```

在IOS-XE C9800 WLC上

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
```

遇到此問題時，AP日誌將顯示與以下類似的錯誤：

在SHA-1 AP上（在2014年中期之前製造）：

```
*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
```

在SHA-2 AP上（2014年中期之後製造）：

```
*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
```

因應措施

如果您沒有運行固定軟體，請按照以下步驟允許IOS AP加入。

1. 禁用NTP，以防止控制器自動設定其時間轉發。

```
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.將WLC上的日期變更為2022年12月4日之前、但2022年11月1日之前的某個日期，因為它可能會使控制器中的證書或更新的AP中的證書失效。

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

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

3.驗證WLC上的時間是否已更改

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

C9800#show clock
00:00:02.573



Fri Dec 2 2022
```

4.等待所有AP以新映像的「已註冊」狀態啟動。

注意：在某些情況下，可能需要在更改日期後重新啟動AP才能加入AP。但是請務必等待至少

30分鐘，以允許AP重新加入，然後再重新啟動AP

5.再次啟用NTP

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

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

6.儲存配置

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

C9800#write memory
```

7.重新驗證WLC上的時鐘

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

升級到固定軟體

在AireOS WLC上

1. 如果有任何存取點在下載中停滯，則請將控制器時間設定為原時間，以便存取點能完成下載並在升級至軟體之前以註冊狀態啟動。
    1. 有關設定回退時間的詳細資訊，請參閱上述解決方法部分

    2. 如果由於操作原因，您無法設定回退時間，則阻止受影響的IOS AP嘗試加入控制器，例如關閉其交換機埠或安裝ACL以阻止CAPWAP。

2. 現在沒有AP處於下載狀態，請確保WLC的時間設定為當前時間（重新啟用NTP）。
3. 在AireOS WLC（8.10.183.0或更高版本）上安裝固定軟體；或者，如果無法從8.5升級，請使用8.5.182.7（如果使用8.5 mainline，或8.5.182.105，用於8.5 IRCM）。請參閱以下連結下載固定軟體。
    - 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（隱藏帖子）

8.5.182.7(8.5 mainline):https://software.cisco.com/download/specialrelease/8f166c6d88b9f77aabb63f78affa9749。

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

4. （可選）在重新啟動之前，將固定軟體預下載到加入的AP。
5. 重新啟動WLC。
6. 如果關閉AP交換機埠或阻止了CAPWAP，請刪除這些塊以允許IOS AP重新加入和升級.

在IOS-XE 9800 WLC上

1.將17.3.6、17.6.4、17.9.2 IOS-XE軟體下載到9800快閃記憶體。請參閱建議的C9800 WLC的IOS-XE版本，以根據您環境中的AP型號和使用中的功能選擇最適合您環境的版本。

2.將17.3.6 APSP7或17.6.4 APSP1或17.9.2 APSP1檔案（帶有IOS AP修復程式）下載到9800快閃記憶體。

- 17.3.6:17.3.6 APSP7，通過CSCwd83653/CSCwe10047（修復程式也包含在APSP2和APSP5中）

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（適用於IW3702），通過CSCwd87305

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（適用於IW3702），通過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

附註：
1)17.3.6 APSP7包括針對多個錯誤的修復(CSCvx32806、CSCwc32182、CSCvz99036、CSCwd37092、CSCwc78435、CSCwc88148)，以及CSCCSC80290
2)17.6.4 APSP1包括針對多個錯誤的修復(CSCwc73090、CSCwc71198、CSCwc78435、CSCwd40731、CSCvx32806)，以及CSCwd80290（用於IW3700）。

3.除非已安裝17.3.6，否則請立即安裝17.3.6 IOS-XE並重新載入。

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

4. 9800重新啟動後 — 如果控制器時間已及時設定，現在將其時間設定為當前（重新啟用NTP）。

5安裝APSP7以恢復IOS AP:

```
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
```

常見問題 (FAQ)

- 我當前註冊的AP是否由於此問題而斷開連線或無法加入？
執行與WLC相同版本的AP將繼續正常運作，不會出現問題，且會正常開機並加入。此問題僅影響作為映像升級一部分完成的映像驗證過程。

- AP預下載是否受到影響？

會。由於AP預下載涉及將映像下載到AP並由AP驗證映像，因此會遇到相同的過期證書和映像驗證失敗。

- 時間的變化會對服務產生什麼影響？客戶能否在中午完成此操作？還是應該安排一個維護視窗，讓其停機並影響服務？
  更改控制器時間對AP加入和無線客戶端連線沒有操作影響。但是，DNA中心保證、CMX和思科(DNA)空間可能會受到影響。一旦加入AP並將時間設定為當前時間，這些服務即可恢復。

- 如果無法重新設定生產控制器上的時間，該怎麼辦？
  使用與生產WLC相同的代碼版本設定臨時WLC（vWLC或9800-CL也可以工作）。恢復臨時WLC上的時間並將AP加入臨時WLC。一旦AP下載代碼並移至臨時WLC上的「已註冊」狀態，請將AP移至生產WLC。

- 是否需要更改安裝固定版本的時間？

只有使用AireOS時，如果AP停滯在下載狀態。有關詳細資訊，請參閱升級到固定軟體一節。

- 如果我新增新的AP會發生什麼情況？
  如果新AP的版本與控制器相同，則AP應能順利加入。
  另一方面，如果版本不匹配，AP將嘗試下載相應的映像。如果控制器上的代碼沒有捆綁的固定AP映像，這將導致AP無法按所述進行升級，因此需要採取解決方法。
  如果控制器已升級到其中一個固定版本，則可以正常新增新AP，並完成升級過程。

- 從RMA收到的單元會發生什麼情況?
  這相當於新增新的AP：如果您正在運行帶有AP映像修復程式的控制器版本，它們將正常加入和升級。
  否則，請應用時間解決方法。

- 我需要保留為操作修改的時間嗎？
  不能，AP完成升級過程後，您可以將控制器設定回當前時間，然後重新啟用NTP。

- 我在AP日誌%PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID上看到此錯誤：證書鏈驗證失敗。證書(SN:xx)尚未生效。有效期從HH:MM:SS UTC Mar 1 2022」開始。這到底是同樣的症狀還是新的症狀？

此錯誤表示WLC上的時鐘設定在2022年3月1日之後，該日期是憑證的開始日期（在此案例中）。此日期因生產WLC的時間或虛擬WLC上生成自簽名證書的時間而異。

修改WLC上的時鐘以使憑證生效。

- 思科如何防止此問題再次發生？
  我們正在完成對所有企業產品的全面稽核，以確定可能未檢測到的任何類似問題，並實施糾正措施
  此外，還對IOS AP映像包流程進行了更改，以更正此問題。

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）。