2022年12月4日之后，由于映像签名证书过期，IOS AP映像下载失败(CSCwd80290)

目录

简介

本文档提供有关IOS接入点(AP)加入失败的详细信息，请参阅AireOS和C9800无线LAN控制器(WLC)在2022年12月4日之后的情况。此问题由Cisco bug CSCwd80290和Field Notice FN72524跟踪，是由AP映像签名证书验证失败引起的。

受影响的产品

此问题影响运行IOS的所有轻量接入点 — 包括：802.11ac Wave 1 AP（IW3702/3700/2700/1700/1570系列）和较早的AP(包括700/1530/1550/3600/2600/3500/AP802/AP8 03系列。受影响的轻量IOS映像的构建时间为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响。 运行AP-COS(802.11ac Wave 2、Wi-Fi 6、Wi-Fi 6E AP)的AP不受影响，IOS AP也不处于自主模式。

问题

当通过CAPWAP升级或降级IOS AP时，在2022年12月4日之后，它们可能会陷入映像下载循环，从而无法加入WLC，因为无法验证下载的映像中的签名证书。

根本原因

捆绑在AP IOS映像中的映像签名证书于2012年12月4日颁发，并于2022年12月4日到期。在AP上安装软件之前，IOS AP使用此证书验证从WLC下载的映像。因此，在2022年12月4日之后，当AP由于软件升级/降级或在运行不同版本的WLC之间移动而下载代码时，AP将无法验证映像并将无限期地保持下载映像循环。所有AireOS和IOS-XE版本均出现问题。

症状

要验证是否遇到此问题，首先在WLC上检查AP是否停滞在“下载”状态。 然后，为了明确识别问题，请通过ssh、telnet或控制台连接到受影响的AP并查看其日志（或查找syslog服务器上的AP日志）。

在AireOS WLC上

在WLC上，show ap image status(AireOS 8.10)会将受影响的AP显示为“下载”状态。

在8.5中，请使用show ap image all，该命令将在“下载”中显示非零数量的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
```

遇到此问题时，AP日志将显示类似于以下内容的错误：

在SHA-1 AP（在2014年中期之前制造）上：

```
*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（2014年年中之后生产）上：

```
*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
```

解决方法

如果您没有运行固定软件，请按照以下步骤允许IOS AP加入。

1. 禁用NTP，以防止控制器自动设置其转发时间。

```
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.将WLC上的日期更改为2022年12月4日之前，但不更改为2022年11月1日之前的某个日期，因为它可能会使控制器或较新AP中的证书失效。

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

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

3.验证WLC上的时间是否已更改

```
(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在新映像中进入已注册状态。

注意：在某些情况下，可能需要在日期更改后重新启动AP才能使AP加入。但是，请务必等待至少30分钟，以允许AP重新加入，然后再重新启动AP

5.再次启用NTP

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

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

6.保存配置

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

C9800#write memory
```

7.重新验证WLC上的时钟

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

升级到固定软件

在AireOS WLC上

1. 如果任何AP在下载过程中滞留，请将控制器时间设置回，以便AP在升级到软件之前可以完成下载并进入注册状态。
    1. 有关设置回溯时间的详细信息，请参阅上述解决方法部分
    2. 如果由于操作原因，您无法设置回退时间，则阻止受影响的IOS AP尝试加入控制器，例如关闭其交换机端口或安装ACL以阻止CAPWAP。
2. 现在没有AP处于下载状态，请确保WLC的时间设置为当前时间（重新启用NTP）。
3. 在AireOS WLC上安装固定软件（8.10.183.0或更高版本；如果无法从8.5升级，请使用8.5.182.7；如果使用8.5 mainline，则使用8.5.182.105，适用于8.5 IRCM。）请参阅以下链接下载固定软件。
    - 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（隐藏帖子）

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. （可选）在重新启动之前，将固定软件预下载到加入的AP。
5. 重新启动 WLC.
6. 如果关闭AP交换机端口或阻止了CAPWAP，请删除阻止以允许IOS AP重新加入和升级.

在IOS-XE 9800 WLC上

1.将17.3.6、17.6.4、17.9.2 IOS-XE软件下载到9800闪存。请参阅推荐的C9800 WLC的IOS-XE版本，以根据您环境中的AP型号和正在使用的功能选择最适合您的环境的版本。

2.将17.3.6 APSP7或17.6.4 APSP1或17.9.2 APSP1文件（带IOS AP修复程序）下载到9800闪存。

- 17.3.6:17.3.6 APSP7，通过CSCwd83653/CSCwe10047（APSP2和APSP5中也提供修复程序）

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

980-80: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（适用于IW3702），通过CSCwd87305

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

980-80: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（适用于IW3702），通过CSCwd87612

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

980-80: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

注意：
1)17.3.6 APSP7包含针对多个漏洞的修复(CSCvx32806、CSCwc32182、CSCvz99036、CSCwd37092、CSCwc78435、CSCwc8148)，以及CSCWD80290
2)17.6.4 APSP1包括针对多个漏洞的修复(CSCwc73090、CSCwc71198、CSCwc78435、CSCwd40731、CSCvx32806)，以及CSCwd80290（适用于IW370）。

3.除非已安装17.3.6，否则请立即安装17.3.6 IOS-XE并重新加载。

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

4.在9800重新启动后 — 如果控制器时间已及时回调，现在将其时间设置为当前（重新启用NTP）。

5安装APSP7以恢复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
```

常见问题解答 (FAQ)

- 当前注册的AP是否由于此问题断开连接或无法加入？
  运行与WLC相同版本的AP将继续正常运行，而不会出现问题，并且会正常启动和加入。此问题仅影响映像升级过程中完成的映像验证过程。

- AP预下载是否受到影响？

Yes.由于AP预下载涉及将映像下载到AP并由AP验证映像，因此会遇到相同的过期证书和映像验证失败。

- 时间变化会对服务产生什么影响？客户能否在中午完成此操作？还是应该安排一个维护窗口，让其停机并影响服务？
  更改控制器时间对AP加入和无线客户端连接没有操作影响。但是，DNA中心保证、CMX和思科(DNA)空间可能会受到影响。一旦AP加入且时间设置为当前时间，这些服务预计会恢复。

- 如果无法在生产控制器上设置时间，该怎么办？
  设置与生产WLC具有相同代码版本的临时WLC（vWLC或9800-CL也适用）。恢复临时WLC上的时间并将AP加入临时WLC。一旦AP下载代码并移至临时WLC上的“已注册”状态，请将AP移至生产WLC。

- 是否需要更改安装固定版本的时间？

只有使用AireOS时，如果AP停滞在下载状态。有关详细信息，请参阅升级到固定软件部分。

- 如果添加新的AP会发生什么情况？
  如果新AP安装在与控制器相同的版本上，则AP应能顺利加入。
  另一方面，如果版本不匹配，则AP将尝试下载相应的映像。如果控制器上的代码没有固定AP捆绑的映像，这将导致AP无法按所述进行升级，并且需要采取解决方法。
  如果控制器已升级到某个固定版本，则可以正常添加新的AP，并完成升级过程。

- 从RMA收到的设备会发生什么情况?
  这等同于添加新的AP：如果您运行带AP映像修复程序的控制器版本，它们将正常加入和升级。
  否则，请应用时间解决方法。

- 我需要保留为操作修改的时间吗？
  否，AP完成升级过程后，您可以将控制器设置回当前时间，然后重新启用NTP。

- 我在AP日志%PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID上看到此错误：证书链验证失败。证书(SN: xx)尚未生效。有效期从HH:MM:SS UTC Mar 1 2022”开始。这是相同的症状还是新的症状？

此错误表示WLC上的时钟设置在2022年3月1日之后，该日期是证书的开始日期（在本例中）。此日期因生产WLC的时间或虚拟WLC上生成自签名证书的时间而异。

修改WLC上的时钟以使证书有效。

- 思科如何防止此问题再次发生？
  我们正在完成对所有企业产品的全面审核，以确定可能未被发现的任何类似问题，并实施纠正措施
  此外，已对IOS AP映像包流程进行了更改，以更正此问题。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。