La descarga de la imagen del IOS AP falla debido a que el certificado de firma de la imagen caducó el 4 de diciembre de 2022 (CSCwd80290)

Contenido

Introducción

Este documento proporciona detalles sobre las fallas de unión del punto de acceso (AP) IOS, vistas con los controladores de LAN inalámbrica (WLCs) AireOS y C9800, después del 4 de diciembre de 2022. Este problema es rastreado por el bug Cisco CSCwd80290 y el aviso de campo FN72524 y es causado por una falla de validación del certificado de firma de la imagen AP.

Productos afectados

Este problema afecta a todos los puntos de acceso ligeros que ejecutan IOS, incluidos los puntos de acceso 802.11ac Wave 1 AP (series IW3702/3700/2700/1700/1570) y los puntos de acceso anteriores, incluidos 700/1530/1550/3600/2600/1600/3500/AP8 Serie 02/AP803. Las imágenes IOS ligeras afectadas se crearon entre diciembre de 2012 y noviembre de 2022. Se ven afectados AireOS, Catalyst serie 9800 y los controladores de acceso convergente. Los AP que ejecutan AP-COS (802.11ac Wave 2, Wi-Fi 6, Wi-Fi 6E AP) no se ven afectados, ni los AP IOS están en modo autónomo.

Problema

Cuando los AP IOS se actualizan o se degradan a través de CAPWAP, después del 4 de

diciembre de 2022, pueden quedar atascados en un loop de descarga de imagen, y por lo tanto no pueden unirse al WLC, debido a una falla al validar el certificado de firma en la imagen descargada.

Causa raíz

Los certificados de firma de imágenes agrupados en las imágenes del IOS de AP se emitieron el 4 de diciembre de 2012 y expiraron el 4 de diciembre de 2022. Los AP del IOS utilizan este certificado para validar la imagen descargada del WLC, antes de instalar el software en el AP. Por lo tanto, después del 4 de diciembre de 2022, cuando un AP descarga el código debido a la actualización/downgrade del software o debido a moverse entre los WLC que ejecutan diferentes versiones, el AP no podrá validar la imagen y permanecerá en un loop de imagen de descarga indefinidamente. El problema se observa en todas las versiones de AireOS e IOS-XE.

Síntomas

Para verificar si se está encontrando con este problema, primero verifique en el WLC para los AP atascados en el estado de la descarga. Luego, para identificar positivamente el problema, ssh, telnet o la consola en los AP afectados y ver sus registros (o buscar registros de AP en su servidor syslog).

En un WLC de AireOS

En el WLC, **show ap image status** (AireOS 8.10) mostrará los AP afectados en el estado "Descargando".

En la versión 8.5, utilice **show ap image all**, que mostrará un número distinto de cero de APs en "Downloading".

```
(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 Flexconnect AP Name
Primary Image Backup Image Status Version Next Retry Time Retry Count Predownload --------------
---- -------------- -------------- -------------- -------------- ---------------- ------------
-------------- 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
```

En un WLC IOS-XE C9800

C9800#show ap summary

```
9800-L#show ap summary AP Name Slots AP Model Ethernet MAC Radio MAC Location Country IP Address
State ------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
- AP2702E 2 2702E 0081.c4fb.2e74 843d.c673.10d0 default location 192.168.202.105 Downloading
```

Los registros de AP mostrarán errores similares a los siguientes cuando se encuentre con este

problema:

En un AP SHA-1 (fabricado antes de mediados de 2014):

```
*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 certificate (SN: XX) has expired. Validity period ended on 21:37:36 UTC Dec 4 2022
*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_hash)
*Dec 6 21:35:24.327: AP image integrity check FAILED
```

En un AP SHA-2 (fabricado después de mediados de 2014):

```
*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 too old last_seq_num : 11116,Received sequence num: 1 distance: -11115
*Dec 6 08:47:20.227: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has
failed. The certificate (SN: XX) has expired. Validity period ended on 21:43:46 UTC Dec 4 2022
*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_hash)
*Dec 6 08:47:20.231: AP image integrity check FAILED
```

Solución Aternativa

Si no está ejecutando un software fijo, siga estos pasos para permitir que los AP IOS se unan.

1. Inhabilite NTP, para evitar que el controlador establezca automáticamente su tiempo de reenvío.

```
AireOS: (AireOS WLC)>show time make a note of all configured NTP servers, and delete each one:
(AireOS WLC)>config time ntp delete
```

2. Cambie la fecha en el WLC a algo antes del 4 de diciembre de 2022 pero no antes del 1 de noviembre de 2022, ya que puede invalidar el certificado en el controlador o en los AP más nuevos.

```
(AireOS WLC)> config time manual 12/02/22 00:00:00 C9800#clock set 00:00:00 2 Dec 2022
```

3. Verifique que la hora en el WLC haya cambiado

```
(AireOS WLC)> show time Time..................................... Fri Dec 2 00:00:02
2022 C9800#show clock 00:00:02.573
```

4. Espere a que todos los APs aparezcan en el estado Registrado con la nueva imagen.

> **Nota: En algunos casos, puede ser necesario un reinicio del AP después del cambio de fecha para que el AP se una. Pero asegúrese de esperar al menos 30 minutos para permitir que el AP se una de nuevo antes de reiniciar los AP**

5. Activar NTP de nuevo

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

6. Guarde la configuración

```
(AireOS WLC)>save config Are you sure you want to save? (y/n) y C9800#write memory
```

7. Vuelva a verificar el reloj en el WLC

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

Actualización a software fijo

En un WLC de AireOS

1. Si tiene algún AP atascado en la descarga, después ajuste el tiempo del controlador atrás para que los AP puedan completar la descarga y venir para arriba en el estado registrado antes de actualizar al software. Consulte la sección anterior para obtener más información sobre cómo establecer el tiempo de vueltaSi, por razones operativas, no puede establecer el tiempo atrás, bloquee los AP IOS afectados para que no intenten unirse al controlador, por ejemplo apagando sus puertos de switch o instalando una ACL para bloquear CAPWAP.
2. Ahora que ningún AP está en el estado de la descarga, asegúrese de que el tiempo del WLC esté fijado a la hora actual (vuelva a habilitar NTP.)
3. Instale el software fijo en el WLC de AireOS (8.10.183.0 o superior; o, si no puede actualizar desde 8.5, use 8.5.182.7, si usa 8.5 línea principal, u 8.5.182.105, para 8.5 IRCM.). Consulte los enlaces siguientes para descargar el software fijo. 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/8.10.183.08. 5 (publicaciones ocultas) 8.5.182.7 (8.5 línea principal): https://software.cisco.com/download/specialrelease/8f166c6d88b9f77aabb63f78affa9749. 8.5.182.105 (8.5 IRCM): https://software.cisco.com/download/specialrelease/bc334964055fbd9440834f008e5aca34.
4. (Opcionalmente) Antes de reiniciar, predescargue el software fijo en los AP unidos.
5. Reboot de WLC.
6. Si apaga los puertos de switch AP o bloquea CAPWAP, quite los bloques para permitir que los AP IOS se vuelvan a unir y actualicen.

En un WLC IOS-XE 9800

1. Descargue el software IOS-XE 17.3.6, 17.6.4, 17.9.2 al flash 9800. Consulte Versiones recomendadas de IOS-XE para WLC C9800 para elegir la versión más adecuada para su entorno según los modelos de AP en su entorno y las funciones en uso.

2. Descargue el archivo 17.3.6 APSP7 o 17.6.4 APSP1 o 17.9.2 APSP1 (con corrección de IOS AP) al flash 9800.

- 17.3.6: 17.3.6 APSP7 a través de CSCwd83653/CSCwe10047 (corrección también incluida en APSP2 y APSP5)

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 (para IW3702) mediante 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 (para IW3702) mediante 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

Nota:
1) 17.3.6 APSP7 incluye correcciones para varios errores (CSCvx32806, CSCwc32182, CSCvz99036, CSCwd37092, CSCwc78435, CSCwc88148) además de CSC50 wd80290
2) 17.6.4 APSP1 incluye correcciones para varios errores (CSCwc73090, CSCwc71198, CSCwc78435, CSCwd40731, CSCvx32806) además de CSCwd80290 (para IW3) 700).

3. A menos que 17.3.6 ya esté instalado, instale 17.3.6 IOS-XE ahora y recargue.

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

4. Después de los reinicios de 9800 - si la hora del controlador se había retrasado en el tiempo, ahora establezca su tiempo en la corriente (vuelva a habilitar NTP).

5 Instale APSP7 para recuperar los AP IOS:

```
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
```

Preguntas frecuentes

- **¿Mis AP registrados actuales se desconectarán o no podrán unirse debido a este problema?**
  Los AP que ejecutan la misma versión que el WLC continuarán funcionando sin problemas y arrancarán y se unirán normalmente. Este problema sólo afecta al proceso de validación de la imagen realizado como parte de una actualización de la imagen.

- **¿Afecta la predescarga de AP?**

Yes. Dado que la predescarga de AP implica la descarga de una imagen a AP y la validación de la imagen por AP, se encuentra el mismo certificado caducado y la falla de validación de la imagen.

- **¿Qué impacto tiene en el servicio el cambio de hora? ¿Puede un cliente hacer esto a mediodía o debería programar una ventana de mantenimiento con algún tiempo de inactividad y algún impacto en los servicios?**
  El cambio de la hora del controlador no tiene impacto operativo en las uniones de AP y la conectividad del cliente inalámbrico. Sin embargo, los espacios DNA Center Assurance, CMX y Cisco (DNA) pueden verse afectados. Una vez que los AP se unen y el tiempo se fija de nuevo a la hora actual, se espera que estos servicios se recuperen.

- **¿Qué sucede si no puedo volver a establecer el tiempo en mi controlador de producción?**
  Configure un WLC provisional (vWLC o 9800-CL también funciona) con la misma versión de código que el WLC de producción. Revertir el tiempo en el WLC provisional y unir los AP al WLC provisional. Una vez que los AP descargan el código y se mueven al estado registrado en el WLC provisional, mueva los AP al WLC de producción.

- **¿Tengo que cambiar el tiempo para instalar la versión corregida?**

Solo con AireOS, si los AP están atascados en estado de descarga.. Consulte la sección *Actualización a software fijo* para obtener más detalles.

- **¿Qué sucede si añado un nuevo AP ?**
  Si el nuevo AP ha instalado en él la misma versión que el controlador, el AP debe unirse sin problemas.
  Por otro lado, si la versión no coincide, el AP intentará descargar la imagen correspondiente. Si el código en el controlador no tiene las imágenes agrupadas del AP fijo, esto hará que el AP falle la actualización como se describe, y la solución alternativa será necesaria.
  Si el controlador se ha actualizado a una de las versiones fijas, los nuevos AP se pueden agregar normalmente y completar el proceso de actualización.

- **¿Qué ocurrirá con las unidades recibidas de RMA?**
  Esto equivale a agregar un nuevo AP: si está ejecutando una versión del controlador con la corrección de la imagen del AP, se unirán y actualizarán normalmente.
  De lo contrario, aplique la solución temporal.

- **¿Es necesario mantener el tiempo modificado para la operación?**
  No, una vez que los AP han completado el proceso de actualización, puede establecer el controlador nuevamente a la hora actual y volver a habilitar NTP.

- **Veo este error en el registro de AP %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Error en la validación de la cadena de certificados. El certificado (SN: xx) aún no es válido El período de validez comienza el 1 de marzo de 2022 en HH:MM:SS UTC". ¿Es el mismo síntoma o un síntoma nuevo?**

Este error indica que el reloj en el WLC se establece detrás del 1 de marzo de 2022, que es la fecha de inicio del certificado (en este caso). Esta fecha variará dependiendo de cuándo se fabricó el WLC o de cuándo se generó el certificado autofirmado en el WLC virtual.

Modifique el reloj en el WLC para hacer el certificado válido.

- **¿Qué está haciendo Cisco para evitar que este problema se repita?**
  Estamos realizando una auditoría completa de todos los productos empresariales para identificar cualquier problema similar que podría haber pasado desapercibido e implementar medidas correctivas
  Además, se han aplicado cambios al proceso de agrupamiento de imágenes de IOS AP para corregir este problema.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).