Download dell'immagine AP IOS non riuscito a causa di un certificato di firma immagine scaduto il 4 dicembre 2022 (CSCwd80290)

Sommario

[Introduzione](#)
[Prodotti interessati](#)
[Problema](#)
[Causa principale](#)
[Sintomi](#)
[Su un WLC AireOS](#)
[Su un WLC IOS-XE C9800](#)
[Su un punto di accesso SHA-1 (prodotto prima della metà del 2014):](#)
[Su un punto di accesso SHA-2 (prodotto dopo la metà del 2014):](#)
[Soluzione alternativa](#)
[Aggiornamento a software fisso](#)
[Su un WLC AireOS](#)
[Su un IOS-XE 9800 WLC](#)
[Domande frequenti (FAQ)](#)

Introduzione

Questo documento fornisce dettagli sui guasti di join dei punti di accesso (AP) IOS, rilevati sia con AireOS che con i Wireless LAN Controller (WLC) C9800, dopo il 4 dicembre 2022. Questo problema viene rilevato dal bug Cisco CSCwd80290 e dalla notifica sul campo FN72524 ed è causato da un errore di convalida del certificato di firma dell'immagine AP.

Prodotti interessati

Questo problema interessa tutti i punti di accesso lightweight che eseguono IOS, tra cui: 802.11ac Wave 1 AP (serie IW3702/3700/2700/1700/1570) e i punti di accesso precedenti, tra cui 700/1530/1550/3600/2600/1600/3500/AP802 serie 33. Le immagini IOS leggere interessate sono state costruite da dicembre 2012 a novembre 2022. il problema riguarda AireOS, Catalyst serie 9800 e Converged Access Controller. Gli access point con AP-COS (802.11ac Wave 2, Wi-Fi 6, Wi-Fi 6E AP) non sono interessati, né gli access point IOS sono in modalità autonoma.

Problema

Quando gli access point IOS vengono aggiornati o declassati tramite CAPWAP, dopo il 4 dicembre 2022, potrebbero rimanere bloccati in un loop di download dell'immagine e quindi non riuscire a collegarsi al WLC, a causa di un errore nella convalida del certificato di firma nell'immagine scaricata.

Causa principale

I certificati di firma delle immagini inclusi nelle immagini AP IOS sono stati rilasciati il 4 dicembre 2012 e sono scaduti il 4 dicembre 2022. Gli access point IOS usano questo certificato per convalidare l'immagine scaricata dal WLC, prima di installare il software sull'access point. Quindi, dopo il 4 dicembre 2022, quando un access point scarica il codice a causa di un aggiornamento/downgrade del software o a causa di uno spostamento tra WLC che eseguono versioni diverse, l'access point non riuscirà a convalidare l'immagine e rimarrà in un loop di immagini di download per un tempo indefinito. Il problema si verifica in tutte le versioni AireOS e IOS-XE.

Sintomi

Per verificare se il problema si è verificato, verificare innanzitutto sul WLC se gli AP sono bloccati nello stato di download. Quindi, per identificare in modo positivo il problema, eseguire il protocollo ssh, telnet o console nei punti di accesso interessati e visualizzarne i log (oppure cercare i log dei punti di accesso sul server syslog).

Su un WLC AireOS

Sul WLC, il comando **show ap image status** (AireOS 8.10) visualizzerà gli access point interessati in stato "Download".

Nella versione 8.5, usare **show ap image** che mostrerà un numero diverso da zero di access point in "Download".

```
(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
```

Su 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
```

Quando si verifica questo problema, nei log dei punti di accesso vengono visualizzati errori simili a quelli riportati di seguito:

Su un punto di accesso SHA-1 (prodotto prima della metà del 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
```

Su un punto di accesso SHA-2 (prodotto dopo la metà del 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
```

Soluzione alternativa

Se non si sta eseguendo software fisso, attenersi alla seguente procedura per consentire l'aggiunta degli IOS AP.

1. Disabilitare NTP per impedire al controller di impostare automaticamente l'ora in avanti.

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

2. Modificare la data sul WLC in una data precedente al 4 dicembre 2022 ma non precedente al 1 novembre 2022, in quanto potrebbe invalidare il certificato nel controller o nei nuovi access point.

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

3. Verificare che l'ora sul WLC sia cambiata

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

4. Attendere che tutti gli access point vengano impostati sullo stato Registrato con la nuova immagine.

> **Nota: in alcuni casi, dopo la modifica della data potrebbe essere necessario riavviare l'access point per aggiungerlo. Tuttavia, attendere almeno 30 minuti per consentire al punto di accesso di tornare indietro prima di riavviare i punti di accesso**

5. Abilitare nuovamente NTP

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

6. Salvare la configurazione

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

7. Verificare nuovamente l'orologio sul WLC

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

Aggiornamento a software fisso

Su un WLC AireOS

1. Se il download è bloccato, impostare il tempo del controller in modo che i punti di accesso possano completare il download e diventare registrati prima di eseguire l'aggiornamento al software. Per ulteriori informazioni sull'impostazione del tempo di ritorno, vedere la sezione precedente relativa alle soluzioni alternativeSe, per motivi operativi, non è possibile impostare il tempo trascorso, bloccare gli IOS AP interessati dal tentativo di collegarsi al controller, ad esempio chiudendo le porte switch o installando un ACL per bloccare CAPWAP.
2. Ora che nessun access point è in stato di download, verificare che l'ora del WLC sia impostata sull'ora corrente (riabilitare NTP).
3. Installare il software fisso sul WLC di AireOS (8.10.183.0 o versione successiva; se non è possibile eseguire l'aggiornamento dalla versione 8.5, usare la versione 8.5.182.7, se si usa la versione 8.5, o la versione 8.5.182.105, per 8.5 IRCM). Fare riferimento ai collegamenti seguenti per scaricare il software fisso. 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 (post nascosti) 8.5.182.7 (linea principale 8.5): https://software.cisco.com/download/specialrelease/8f166c6d88b9f77aabb63f78affa9749. 8.5.182.105 (8.5 IRCM): https://software.cisco.com/download/specialrelease/bc334964055fbd9440834f008e5aca34.
4. (Facoltativo) Prima del riavvio, eseguire il predownload del software fisso sui punti di accesso collegati.
5. Riavviare il WLC.
6. Se si arrestano le porte di commutazione AP o si blocca CAPWAP, rimuovere i blocchi per consentire agli access point IOS di unirsi nuovamente e aggiornare.

Su un IOS-XE 9800 WLC

1. Scaricare il software IOS-XE 17.3.6, 17.6.4, 17.9.2 su 9800 flash. Per scegliere la versione più adatta al proprio ambiente, in base ai modelli AP in uso e alle funzionalità in uso, consultare le versioni IOS-XE consigliate per i WLC C9800.

2. Scaricare il file 17.3.6 APSP7 o 17.6.4 APSP1 o 17.9.2 APSP1 (con correzione dell'access point IOS) su 9800 flash.

- 17.3.6: 17.3.6 APSP7 tramite CSCwd83653/CSCwe10047 (correzione inclusa anche in APSP2 e 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 (per IW3702) tramite 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 (per IW3702) via 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 include correzioni per bug multipli (CSCvx32806, CSCwc32182, CSCvz9036, CSCwd37092, CSCwc78435, CSCwc88148) oltre a CSCwd802 90
2) 17.6.4 APSP1 include correzioni per bug multipli (CSCwc73090, CSCwc71198, CSCwc78435, CSCwd40731, CSCvx32806) oltre a CSCwd80290 (per IW3700) .

3. A meno che la versione 17.3.6 non sia già installata, installare la versione 17.3.6 di IOS-XE e ricaricarla.

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

4. Dopo il riavvio di 9800 - se l'ora del controller era stata impostata in tempo, ora impostarla su corrente (riattivare NTP).

5 Installare APSP7 per ripristinare gli access point 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
```

Domande frequenti (FAQ)

- **Gli access point registrati correnti si disconnetteranno o non verranno aggiunti a causa di questo problema?**
  I punti di accesso che eseguono la stessa versione del WLC continueranno a funzionare senza problemi e si avvieranno e si uniranno normalmente. Questo problema influisce solo sul processo di convalida dell'immagine eseguito come parte di un aggiornamento dell'immagine.

- **L'operazione di predownload del punto di accesso è interessata?**

Sì. Dal momento che il predownload comporta il download di un'immagine nel punto di accesso e la convalida dell'immagine da parte del punto di accesso, si verifica lo stesso errore di convalida dell'immagine e del certificato scaduto.

- **Qual è l'impatto del cambiamento di orario sul servizio? Un cliente può farlo a mezzogiorno o deve pianificare una finestra di manutenzione con tempi di inattività e impatto sui servizi?**
  La modifica dell'ora del controller non ha alcun impatto operativo sui join AP e sulla connettività dei client wireless. Tuttavia, DNA Center Assurance, CMX e Cisco (DNA) Spaces potrebbero risentirne. Una volta aggiunti i punti di accesso e ripristinata l'ora corrente, è previsto il ripristino di questi servizi.

- **Cosa succede se non è possibile impostare l'ora sul controller di produzione?**
  Configurare un WLC di gestione temporanea (funziona anche vWLC o 9800-CL) con la stessa versione di codice del WLC di produzione. Ripristinare l'ora sul WLC di gestione temporanea e aggiungere gli AP al WLC di gestione temporanea. Una volta che gli AP hanno scaricato il codice e sono passati allo stato Registrato sul WLC di gestione temporanea, spostare gli AP sul WLC di produzione.

- **È necessario modificare l'ora di installazione della versione fissa?**

Solo con AireOS, se gli access point sono bloccati nello stato di download. Fare riferimento alla sezione sull'*aggiornamento al software fisso* per ulteriori dettagli.

- **Cosa succede se si aggiunge un nuovo punto di accesso?**
  Se il nuovo access point ha installato la stessa versione del controller, l'access point dovrebbe unirsi senza problemi.
  D'altra parte, se la versione non corrisponde, l'access point proverà a scaricare l'immagine corrispondente. Se il codice sul controller non dispone di immagini fisse dell'access point in bundle, l'aggiornamento dell'access point non riuscirà come descritto e sarà necessaria una soluzione alternativa.
  Se il controller è stato aggiornato a una delle versioni fisse, è possibile aggiungere normalmente nuovi access point e completare il processo di aggiornamento.

- **Cosa succede alle unità ricevute da RMA?**
  Equivale ad aggiungere un nuovo punto di accesso: se si esegue la versione del controller con la correzione dell'immagine del punto di accesso, il punto di accesso verrà aggiunto e aggiornato normalmente.
  In caso contrario, applicare la soluzione alternativa.

- **È necessario modificare l'ora per l'operazione?**
  No, una volta che gli access point hanno completato il processo di aggiornamento, è possibile ripristinare l'ora corrente del controller e riattivare l'NTP.

- **Questo errore si verifica nel registro AP %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: convalida della catena di certificati non riuscita. Il certificato (SN: xx) non è ancora valido. Il periodo di validità inizia il giorno HH:MM:SS UTC Mar 1 2022. È lo stesso sintomo o un nuovo sintomo?**

Questo errore indica che l'orologio sul WLC è impostato prima del 1 marzo 2022, che è la data di inizio del certificato (in questo caso). La data varia a seconda di quando il WLC è stato prodotto o di quando è stato generato il certificato autofirmato sul WLC virtuale.

Modificare l'orologio sul WLC per rendere valido il certificato.

- **Cosa sta facendo Cisco per evitare che il problema si ripeta?**
  Stiamo completando un audit completo su tutti i prodotti Enterprise, per identificare eventuali problemi simili che non sarebbero stati rilevati e implementare le azioni correttive
  Per risolvere il problema, sono state inoltre applicate modifiche al processo di aggregazione delle immagini di IOS AP.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).