

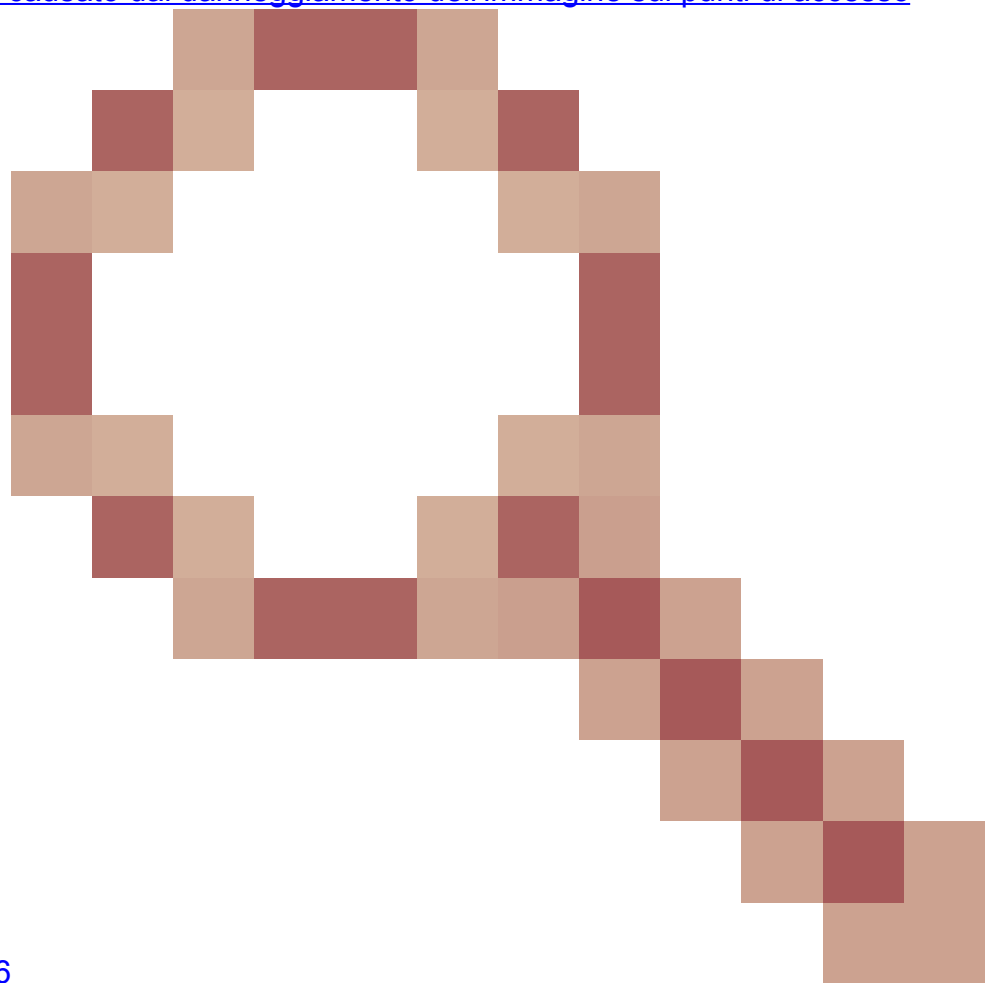
Aggiornamento Sicuro Dei Punti Di Accesso, Evitando Il Danneggiamento Dell'Immagine Che Causa Il Loop Di Avvio

Sommario

Introduzione

Alcuni access point Cisco (AP) possono scaricare un'immagine danneggiata tramite CAPWAP da un controller serie 9800. A seconda della versione del software dell'access point, l'access point potrebbe tentare di avviare l'immagine danneggiata, creando un loop di avvio. Questo articolo spiega quali modelli AP e quali percorsi di rete sono soggetti al danneggiamento delle immagini e come eseguire l'aggiornamento in modo sicuro.

Se i punti di accesso si trovano in un loop di avvio a causa di questo problema, vedere l'articolo [Ripristino da un loop di avvio causato dal danneggiamento dell'immagine sui punti di accesso](#)



[Wave 2 e 11ax \(CSCvx32806](#)

) per istruzioni sulle procedure di ripristino.

Come stabilire se un aggiornamento può danneggiare l'immagine

I punti di accesso possono essere soggetti al download di software danneggiato e al tentativo di avviarlo, se le seguenti condizioni riguardano la distribuzione:

Prodotti non interessati

- Wireless LAN Controller (WLC): il download di access point dai Wireless LAN Controller di AireOS non è interessato
- Mobility Express, controller wireless integrato
- AP - Aironet serie 1800/1540/1100AC Wave 2 11ac AP e Wave1 11ac Access Point (1700/2700/3700/1570/IW3700) non sono interessati (anche se questi AP sono registrati a 9800 WLC, non ne è influenzato l'impatto)
- AP Wi-Fi 6E introdotti dal 2023: IW9167, IW9165, C9163

Prodotti interessati

- WLC: il download dei punti di accesso da Cisco Catalyst serie 9800 Wireless LAN Controller potrebbe essere interessato
- AP: i seguenti modelli AP che eseguono la registrazione ai Cisco Catalyst serie 9800 Wireless LAN Controller sono interessati:
 - Access point Aironet Wave2 11ac (2800/3800/4800/1560/IW6330/ESW6300)
 - Access point Catalyst serie 9100 Wi-Fi6 (9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
 - Access point Catalyst serie 9100 Wi-Fi6E (9136/9162/9164/9166)

Versioni interessate: la sindrome dell'avvio di un'immagine non valida

Il problema, ossia il tentativo da parte del punto di accesso di avviare un'immagine danneggiata, viene risolto dai seguenti ID bug Cisco: [CSCvx32806](#), [CSCwc72021](#), [CSCwd90081](#), risolti nelle seguenti versioni:

- 8.10.185.0 e superiori
- 17.3.7 e oltre
- 17.6.6 e oltre
- 17.9.3 e oltre
- 17.11.1 e oltre

Una volta che il punto di accesso è aggiornato al software con le correzioni di cui sopra, potrebbe comunque scaricare un'immagine danneggiata; tuttavia, non tenterà di avviare quell'immagine, ma continuerà a tentare di nuovo il download fino a che non riesce.

Percorsi di rete interessati

Il problema di danneggiamento dell'immagine del punto di accesso non è stato rilevato con un

percorso LAN tra il 9800 e i punti di accesso, ossia i percorsi con una MTU IP completa di 1500 byte, con bassa latenza e bassissima perdita di pacchetti. Il problema si verifica con maggiore probabilità sui tunnel CAPWAP su una WAN, con le seguenti caratteristiche del percorso:

- perdita di pacchetti elevata
- MTU CAPWAP bassa (inferiore a 1485 byte): più bassa è la MTU, maggiore è il rischio
 - una MTU CAPWAP bassa può essere un sintomo di perdita di pacchetti

Come Stabilire Se Il Percorso Di Rete È A Rischio

- Sul modello 9800, controllare l'MTU del percorso CAPWAP con

```
<#root>
```

```
9800-L#show capwap detailed
```

```
Name          APMAC          SourceIP          SrcPort  DestIP          DestPort
```

```
MTU
```

```
Mode          McastIf
```

```
-----  
Capwap1       D4AD.BDA2.8240 192.168.203.203 5247    192.168.6.100  5248
```

```
1485
```

```
multicast Mc1
```


```
Capwap2       084F.F983.4A40 192.168.203.203 5247    192.168.6.103  5253
```


```
1005
```

```
multicast Mc1
```

- Se l'MTU di un determinato punto di accesso sta fluttuando, si tratta di un forte indicatore di rischio
- Oppure **mostra la configurazione dell'access point in generale | include CAPWAP\ Percorso\ MTU** (in show tech-support wireless)
 - Usare [Wireless Config Analyzer Express \(WCAE\)](#) sull'output "show tech-support wireless" dello switch 9800 per verificare l'MTU degli access point in Access Point > Configurazione
- Sul modello 9800, usare "show ap uptime" e cercare gli access point con un lungo "tempo di operatività" e un breve "tempo di operatività dell'associazione"
 - Se non vi è alcun motivo per cui gli access point abbiano un breve tempo di operatività dell'associazione (ad esempio, nessuna riconfigurazione), ciò potrebbe indicare un percorso di rete a rischio

Come eseguire un aggiornamento sicuro da una versione non fissa del software AP

 Nota: se la distribuzione è suscettibile di danneggiamento dell'immagine (ad esempio modelli AP interessati, esecuzione di software senza la correzione per la sindrome di avvio da immagine errata, con caratteristiche WAN a rischio), non eseguire l'aggiornamento

 aggiornando semplicemente il software 9800 e facendo sì che gli AP si uniscano nuovamente e scarichino il nuovo software - potrebbero essere soggetti al danneggiamento dell'immagine e all'immissione di un loop di avvio. Utilizzare invece uno dei metodi seguenti:

Aggiornamento ai punti di accesso tramite WLC locale

Se possibile, posizionare un controller di gestione temporanea sulla LAN degli access point, ad esempio un access point 9800-CL o (per gli access point Wave 2/Wi-Fi 6) un access point in modalità EWC, quindi aggiornare gli access point alla versione di destinazione. In tal modo, essi potranno collegarsi al controller di produzione senza rischi.

Aggiornamento tramite controller AireOS

Se si dispone di un controller AireOS con versione 8.10.190.0 o successiva e se i modelli AP sono supportati da AireOS, collegare gli AP al controller. In questo modo gli access point verranno aggiornati al software fisso e potranno essere collegati al controller di produzione in modo sicuro.

Aggiornamento tramite download archivio-sw

Posizionare nell'area intermedia le immagini AP di destinazione su un server TFTP / SFTP accessibile agli access point di aggiornamento. Gli aggiornamenti delle immagini AP tramite TFTP o SFTP non sono soggetti al problema di danneggiamento delle immagini. I punti di accesso possono avviare una richiesta di download delle immagini dalla CLI del controller o (se i punti di accesso sono collegati al controller) dalla CLI del controller.

1. Configurare un server TFTP o SFTP in una posizione accessibile agli access point. Si noti che le prestazioni TFTP sono gestite dalla latenza, pertanto i download saranno lenti se il server TFTP è remoto dagli access point. Poiché SFTP utilizza il TCP, la sua velocità di trasmissione sarà notevolmente superiore se si utilizza un percorso ad alta latenza. Tuttavia, SFTP non può essere attivato dal WLC, in quanto richiede una finestra di dialogo interattiva per immettere il nome utente e la password.
2. Posizionare nell'area intermedia l'immagine o le immagini AP desiderate su un server TFTP o SFTP. [Vedere la Tabella 4 nella](#) matrice di [compatibilità](#) per la versione AP 15.3(3)J* che mappa alla versione IOS-XE desiderata, quindi scaricare le immagini appropriate del software Lightweight AP per i modelli AP interessati [da software.cisco.com](http://software.cisco.com).
 1. Ad esempio, l'immagine AP 17.9.5 per CW9162 [isap1g6b-k9w8-tar.153-3.JPN4.tar](#).
3. Per eseguire l'aggiornamento tramite AP CLI: se AP CLI è accessibile tramite console o SSH:

1. Immettere il comando TFTP o SFTP:

```
archive download-sw /no-reload tftp://<indirizzo-ip>/<immagine>  
o  
archive download-sw /no-reload sftp://<indirizzo-ip>/<immagine>  
Nome utente:USER  
Password:XXX
```

L'immagine danneggiata verrà sovrascritta con l'immagine valida.

2. Una volta completato il download dell'immagine, emettere:

test di riavvio capwap

Il processo CAPWAP verrà riavviato in modo che l'access point riconosca l'immagine appena installata.

3. Per aggiornare un numero elevato di access point tramite "archive download-sw", invece di immettere il comando in ciascun access point singolarmente, è possibile utilizzare un metodo di script. Vedere di seguito Aggiornamento dei punti di accesso tramite il controller WLAN.
4. Se gli AP sono collegati a un controller, è possibile aggiornarli dalla CLI del controller (solo TFTP):
 1. In IOS-XE: **nome ap APNAME tftp-downgrade ip.addr.of.server nomeimmagine.tar**
 2. In AireOS: **config ap tftp-downgrade ip.addr.of.server nomeimmagine.tar APNAME**
 1. Sebbene i download CAPWAP da AireOS non siano soggetti a danneggiamento dell'immagine, se si intende eseguire la migrazione degli access point da AireOS a 9800, è necessario prima scaricare un'immagine AP con le correzioni per Alt-boot e Sindrome di avvio di un'immagine non valida (8.10.190.0 o superiore), prima di unire gli access point a 9800.
 3. Monitorare i registri del server TFTP o SFTP per verificare che ciascun punto di accesso abbia scaricato correttamente l'immagine. Una volta completato il download, ogni access point si ricarica, eseguendo l'immagine appena scaricata.

Aggiornamento degli access point tramite predownload, monitoraggio degli errori

Caricare l'immagine di destinazione sul modello 9800 e utilizzare la funzione di predownload del punto di accesso per inviare la nuova immagine sul punto di accesso, monitorando al contempo le istanze di danneggiamento dell'immagine del punto di accesso.

Passaggio 1. Verificare che SSH sia abilitato nei profili di join AP sul WLC del C9800. Configurare un server syslog nella rete. Configurare l'indirizzo IP del server syslog in Profilo di join AP per tutti gli elementi e impostare il valore di log trap su Debug. Verificare che il server syslog riceva syslog dal punto di accesso.

Edit AP Join Profile

General Client CAPWAP AP **Management** Security ICap QoS

Device User Credentials CDP Interface

TFTP Downgrade

IPv4/IPv6 Address

Image File Name

System Log

Facility Value

Host IPv4/IPv6 Address

Log Trap Value

Secured

Telnet/SSH Configuration

Telnet

SSH

Serial Console

AP Core Dump

Enable Core Dump

Passaggio 2. Scaricare l'immagine software nel WLC del C9800 per prepararlo per il predownload tramite CLI:

```
C9800# copy tftp://x.x.x.x/C9800-80-universalk9_wlc.17.03.07.SPA.bin bootflash:  
C9800# install add file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
```

Passaggio 3. Eseguire il pre-download dell'immagine AP sui WLC di Cisco C9800:

```
C9800# ap image predownload
```

Nota: a seconda della scala e del tipo di distribuzione, questa operazione può richiedere da pochi minuti ad alcune ore. Non riavviare il controller o i punti di accesso finché non viene verificata la validità delle immagini.

Passaggio 4. Una volta completato il pre-download per tutti gli access point, verificare la presenza di uno di questi due messaggi di log sul server syslog:

- La firma dell'immagine ha avuto esito positivo.

- Errore di verifica della firma dell'immagine: -3

Controllare inoltre l'output del comando `show ap image summary`, verificando la presenza di eventuali istanze di Failed to Download (Impossibile scaricare). Se il contatore è diverso da zero, individuare gli access point con errori tramite l'immagine `show ap | include Failed`.

Attenzione: in caso di errore di verifica della firma dell'immagine del log dei punti di accesso o di mancato download dei punti di accesso, **NON PROCEDERE OLTRE CON IL PROCESSO DI AGGIORNAMENTO**. Se in tutti i punti di accesso è visualizzato il messaggio "Verifica riuscita della firma dell'immagine", tutti i punti di accesso hanno scaricato correttamente l'immagine ed è possibile procedere con l'aggiornamento a 9800 senza problemi.

Passaggio 5. Se in uno dei punti di accesso si è verificato un errore di verifica o il download non è riuscito, per evitare un loop di avvio è necessario sovrascrivere l'immagine nella partizione di backup del punto di accesso con un archivio che scarica un'immagine del punto di accesso separata, utilizzando il processo seguente.

Se il numero di punti di accesso non funzionanti è ridotto, è sufficiente eseguire il protocollo SSH su ciascun punto di accesso e procedere come segue.

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

Nota: è necessario il riavvio del test capwap in modo che il processo CAPWAP dell'access point riconosca che l'immagine nella partizione di backup è stata aggiornata. Ciò causerà una breve interruzione del servizio, poiché la connessione CAPWAP con lo switch 9800 viene riavviata. Se si tratta di un problema operativo, questo passaggio può essere posticipato a una finestra di manutenzione.

Aggiorna i punti di accesso tramite il controller WLAN

Se il numero di access point da aggiornare tramite `download-sw` di archivio è elevato, è possibile usare un processo automatizzato usando il [controller WLAN](#).

Passaggio 1a. Installare il controller WLAN su un computer Mac o [Windows](#).

Passaggio 1b. Popolare il file csv `aplist` con i relativi punti di accesso non funzionanti.

Passaggio 1c. Popolare il file `cmdlist` con i seguenti comandi (è sempre possibile aggiungerne altri a propria discrezione):

```
COS_AP#term mon
```

```
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

Passaggio 1d. Eseguire il controller WLAN.

Passaggio 1e. Una volta completata l'esecuzione, controllare tutti i file di log dell'access point per verificare che l'operazione sia stata completata correttamente.

Passaggio 2. Attivare immediatamente l'immagine sul WLC del C9800 e ricaricarla.

```
C9800#install activate file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
- Confirm reload when prompted
```

Passaggio 3. Eseguire il commit dell'immagine sul WLC C9800. Se si ignora questo passaggio, WLC eseguirà il rollback all'immagine software precedente

```
C9800#install commit
```

Domande frequenti

D. Ho eseguito un predownload qualche giorno fa, ma non ho ancora riavviato i miei Cisco C9800 WLC e AP. Non si dispone di syslog per verificare se l'immagine è danneggiata. Come verificare se l'immagine è danneggiata?

R. Selezionare `show logging` su access point/syslog. se nell'output del comando `show logging` non vengono visualizzati messaggi di esito positivo o negativo, è possibile utilizzare il comando `"show flash syslogs"` per archiviare l'output del comando `syslog` da quando è stato eseguito il predownload. Se viene visualizzato il messaggio "Verifica riuscita della firma dell'immagine", significa che il punto di accesso ha scaricato l'immagine correttamente.

D: Ho un'installazione centralizzata con i punti di accesso in modalità locale. È ancora necessario eseguire i passaggi elencati nella sezione Soluzioni/Soluzioni?

R: Questo problema è stato segnalato solo quando si aggiornano gli access point su una connessione WAN. È molto improbabile che i punti di accesso in modalità locale e sulle reti locali incontrino questo problema, quindi non è necessario seguire questa procedura per gli aggiornamenti, se si è certi che ci sia una perdita di pacchetti molto ridotta tra il controller e i punti di accesso.

D: Ho nuovi punti di accesso non inclusi. Come è possibile distribuirli senza che si verifichi questo

problema?

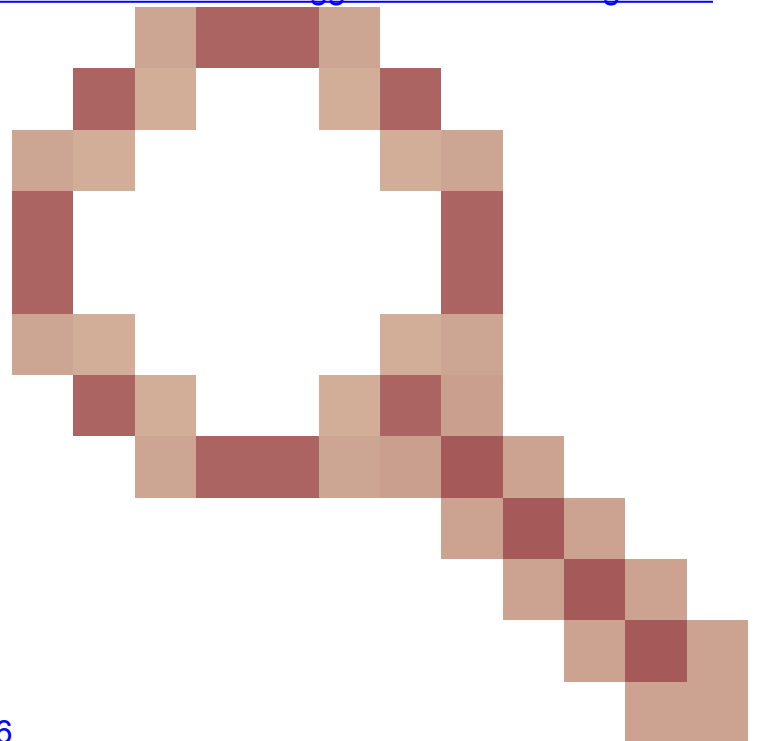
R: Anche i nuovi access point non inclusi che scaricano codice sulla WAN saranno soggetti a questo problema, a meno che non siano stati prodotti dopo dicembre 2023.

D: Cosa sta facendo Cisco a lungo termine per risolvere questo problema con i download di immagini CAPWAP dallo switch 9800 che vengono danneggiati?

R: Se la versione 17.11 o successiva dell'access point è già in esecuzione, è possibile usare la funzione di download delle immagini fuori banda per estrarre l'immagine dal controller usando HTTPS. Il TCP trasmette i dati in modo affidabile, utilizzando una finestra scorrevole - quindi è anche molto più veloce su una WAN, rispetto al CAPWAP (o TFTP)

D: I punti di accesso sono ora in loop. Come è possibile ripristinarli?

R: Vedere l'articolo [Ripristino da un loop di avvio causato dal danneggiamento dell'immagine sui](#)



[punti di accesso Wave 2 e 11ax \(CSCvx32806](#)

[\).](#)

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).