# Ripristino dei punti di accesso C9105AXW con blocchi danneggiati nella memoria flash

## Sommario



## Introduzione

Un certo numero di access point C9105AXW (tutti i PID) sono stati prodotti con un sottosistema flash NAND che potrebbe, nel tempo, contrassegnare spudoratamente i blocchi come danneggiati. Una volta contrassegnati 94 blocchi come danneggiati, la tabella dei blocchi errati flash è piena. Di conseguenza, l'AP può presentare diversi sintomi:

- Il file system flash potrebbe diventare writelocked, pertanto l'access point non è più in grado di eseguire il commit delle modifiche di configurazione, scrivere nuovi log o scaricare una nuova immagine. Si possono verificare errori simili a quelli riportati di seguito:
  sync_log: impossibile aprire /storage/syslogs/7: file system di sola lettura
- L'access point potrebbe bloccarsi a causa di un errore del kernel che mostra errori UBIFS simili a quelli riportati di seguito:
  <3>[02/06/2023 05:06:06.0290] Errore UBIFS (ubi0:1 pid 5454): do_writepage: impossibile scrivere la pagina 8 del codice inode 54848, errore -30
- L'access point potrebbe non essere in grado di avviarsi; nel log della console viene visualizzato un errore simile al seguente:
  [01/01/1970 00:00:05.0600] errore ubi0: ubi_eba_init: eraseblock fisico insufficiente (0, necessario 1)
  [*01/01/1970 00:00:06.4720] errore di montaggio

In alcuni casi, potrebbe essere necessario sostituire l'access point.

Cisco ha implementato due correzioni per risolvere questo problema.

## Correzioni

### ID bug Cisco CSCwf50177 C9105AXW - numero elevato di blocchi danneggiati

Questo bug impedisce che i blocchi flash vengano erroneamente contrassegnati come danneggiati. Tuttavia, non ripara i punti di accesso che hanno già un numero eccessivo di blocchi danneggiati.

### ID bug Cisco CSCwf68131 Monitoraggio e riparazione di blocchi danneggiati C9105AXW

Questo bug corregge i punti di accesso con blocchi danneggiati eccessivi. Al momento dell'avvio (in modalità u-boot), se la tabella dei blocchi danneggiati del punto di accesso supera il numero di voci di soglia (impostazione predefinita: 40; controllata dalla variabile u-boot SCRUB_LIMIT), la tabella dei blocchi danneggiati viene svuotata prima dell'avvio del punto di accesso.

## Unità interessate

Il problema riguarda solo i punti di accesso C9105AXW, nessun altro modello. Per verificare se sono state specificate unità C9105AXW, aprire l'ID bug Cisco CSCwf50177 in BST e fare clic su "Check Bug Applicability" (Verifica applicabilità bug) per immettere i numeri di serie degli access point.

## Software fisso

Se il problema riguarda i C9105AXW, aggiornare il software con le correzioni per **entrambi gli** ID bug Cisco CSCwf50177 e ID bug Cisco CSCwf68131 . Tenere traccia di quest'ultimo bug per verificare la disponibilità delle correzioni nelle diverse sezioni. Dal 5 settembre 2023, le correzioni sono o saranno disponibili nelle seguenti versioni:

### AireOS

- 8.10 MR10 EFT (8.10.189.111 o superiore - disponibile ora; 8.10 MR10 CCO release prevista per fine settembre/ottobre 2023)
- 8.10 MR9 ESC (8.10.185.7 o superiore - disponibile da TAC now)

### Cisco IOS® XE

- 17.3.7 APSP5 o superiore (richiesta TAC aperta)
- 17.3.8 (CCO fine settembre/ottobre 2023)
- 17.6.5 APSP5 o superiore (su CCO)
- 17.6.6 (CCO fine settembre/ottobre 2023)
- 17.9.3 APSP5 o superiore (su CCO)
- 17.9.4 APSP1 o superiore (su CCO)
- 17.9.5 (CCO 2024)
- 17.12.2 (CCO novembre 2023)
- 17.13.1 (CCO dicembre 2023)

## Controllo dei punti di accesso sensibili per l'esistenza di blocchi danneggiati eccessivi

Innanzitutto, controllate tutti i vostri C9105AXW sensibili, per vedere quanti blocchi cattivi hanno. Se nessuno dei blocchi presenta più di 60 blocchi danneggiati, è possibile eseguire l'aggiornamento direttamente.

### Controllo dei blocchi danneggiati - versione 17.6 e successive

Su ciascun C9105AXW sensibile (come determinato da "Check Bug Applicability" per CSCwf50177) ), raccogliere l'output di "**show flash statistics**". Cercare "conteggio delle eraseblock fisiche errate". Per automatizzare il controllo di un numero elevato di access point, usare il poller WLAN.

### Controllo dei blocchi danneggiati - 8.10 e 17.3

TAC (o altro dipendente Cisco con accesso SWIMS) dovrà essere installato in ciascun C9105AXW sensibile ed eseguire il seguente comando:

```
ubinfo -a
```

Cercare "conteggio delle eraseblock fisiche errate". Per automatizzare il controllo di un numero elevato di punti di accesso, utilizzare RADKit.

## Procedura di aggiornamento

Se le unità C9105AXW sono state interessate da blocchi danneggiati eccessivi, eseguire la procedura seguente durante l'aggiornamento al software fisso.

### Aggiornamento in un'installazione con un solo controller: immagine completa del nuovo controller

1. (Facoltativo) è possibile installare la nuova immagine del controller, ma **non** attivarla e **non** prescaricare il nuovo software AP sui C9105AXW interessati.

2. Continuando a utilizzare la **vecchia** immagine del controller, riavviare i C9105AXW interessati. Nella maggior parte dei casi, ciò consente l'aggiornamento dei punti di accesso interessati. (In alcuni casi, potrebbe essere necessario sostituire alcuni access point)

3. Se lo si desidera, è possibile prescaricare la nuova immagine PA.

4. Ricaricare il controller, eseguendo il nuovo software

### Aggiornamento in un'installazione con un solo controller - APSP

1. (Facoltativo) è possibile installare il nuovo APSP, ma **non** attivarlo e **non** prescaricare il nuovo software AP sui C9105AXW interessati.

2. Riavviare i C9105AXW interessati. Nella maggior parte dei casi, ciò consente l'aggiornamento dei punti di accesso interessati. (In alcuni casi, potrebbe essere necessario sostituire alcuni access point)

3. A questo punto è possibile prescaricare, attivare ed eseguire il commit dell'APSP.

### Aggiornamento in una distribuzione N+1

In questo scenario, viene utilizzato un controller di backup per aggiornare i C9105AXW interessati.

1. Mentre i punti di accesso interessati sono ancora collegati al vecchio controller, aggiornare il controller di backup al software fisso (versione controller completa o APSP)

2. Ricaricare i punti di accesso interessati. Farli ricongiungere al vecchio controller. (In alcuni casi,

potrebbe essere necessario sostituire alcuni access point)

3. Riconfigurare ora i punti di accesso interessati, in modo da impostare il controller primario su quello aggiornato, e farli unire al controller di backup.

4. Dopo aver aggiornato il controller primario al software fisso, è possibile riportare i C9105AXW al controller fisso.

---

# 8.10 Disponibilità di MR10 EFT

Modulo di iscrizione: http://cs.co/810MR10-EFT-Signup

Note release: https://www.cisco.com/web/software/280926587/165753/Release_Notes_8_10_189_111.pdf

**8.10.189.111 Collegamenti per il download di EFT (8.10.189.11)**
8540 Wireless Controller
5520 Wireless Controller
Controller wireless 3504
Controller wireless virtuale
Mobility Express 1815
Mobility Express 1850
Mobility Express 3800
Mobility Express 2800
Mobility Express 4800

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).