

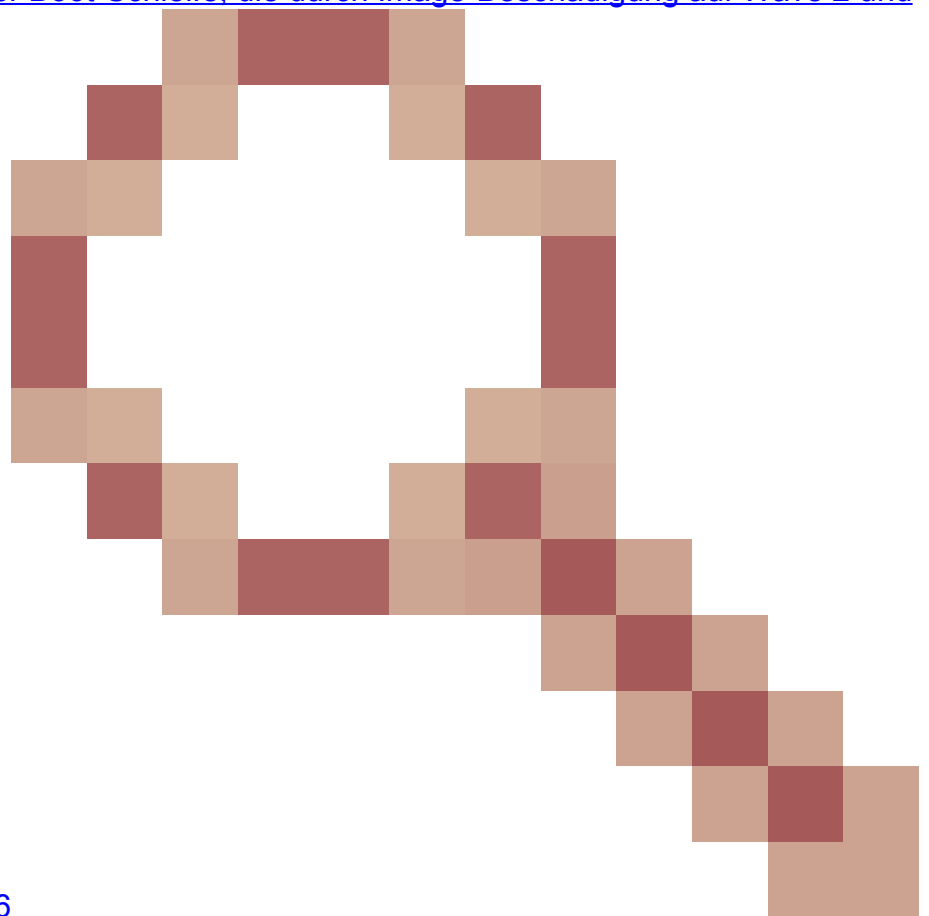
Sicheres Upgrade von Access Points zur Vermeidung von Image-Beschädigungen, die zu Bootschleifen führen

Inhalt

Einleitung

Einige Cisco Access Points (APs) laden möglicherweise beschädigte Images über CAPWAP von einem Controller der Serie 9800 herunter. Je nach Softwareversion des Access Points versucht der Access Point möglicherweise, das beschädigte Image zu booten, was zu einer Bootschleife führt. In diesem Artikel wird erläutert, welche AP-Modelle und welche Netzwerkpfade anfällig für Image-Beschädigungen sind und wie ein sicheres Upgrade durchgeführt werden kann.

Wenn sich Ihre APs aufgrund dieses Problems nun in einer Boot-Schleife befinden, finden Sie im Artikel [Wiederherstellung von einer Boot-Schleife, die durch Image-Beschädigung auf Wave 2 und](#)



[11ax Access Points \(CSCvx32806](#)

[\)](#) verursacht wurde. Hinweise zu Wiederherstellungsschritten.

So erkennen Sie, ob ein Upgrade anfällig für Image-

Beschädigungen ist

Ihre APs können möglicherweise beschädigte Software herunterladen und dann versuchen, diese Software zu starten, wenn die folgenden Bedingungen für Ihre Bereitstellung zutreffen:

Nicht betroffene Produkte

- Wireless LAN Controller (WLCs): APs, die von AireOS Wireless LAN Controllern heruntergeladen werden, sind nicht betroffen.
- Mobility Express, integrierter Wireless-Controller
- APs - Aironet 1800/1540/1100AC-Serie Wave 2 11ac APs und Wave1 11ac Access Points (1700/2700/3700/1570/IW3700) sind nicht betroffen (selbst wenn diese APs sich bei 9800 WLCs registrieren, sind sie davon nicht betroffen).
- Wi-Fi 6E APs, die seit 2023 eingeführt wurden: IW9167, IW9165, C9163

Betroffene Produkte

- WLC : Möglicherweise betroffen sind APs, die von Cisco Catalyst Wireless LAN-Controllern der Serie 9800 heruntergeladen werden.
- APs : Die folgenden AP-Modelle, die für Cisco Catalyst Wireless LAN-Controller der Serie 9800 registriert werden, sind betroffen:
 - Aironet Wave2 11ac Access Points (2800/3800/4800/1560/IW6330/ESW6300)
 - Catalyst Wi-Fi6 Access Points der Serie 9100 (9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
 - Catalyst 9100 Wi-Fi6E Access Points (9136/9162/9164/9166)

Betroffene Versionen: Das Boot-a-Bad-Image-Syndrom

Dieses Problem wird durch die folgenden Cisco Bug-IDs behoben: [CSCvx32806](#), [CSCwc72021](#), [CSCwd90081](#), die in den folgenden Versionen behoben sind. :

- 8.10.185.0 und höher
- 17.3.7 und höher
- 17.6.6 und höher
- 17.9.3 und höher
- 17.11.1 und höher

Nach dem Upgrade des Access Points auf die Software mit den oben genannten Patches wird möglicherweise immer noch ein beschädigtes Image heruntergeladen. Es wird jedoch nicht versucht, dieses Image zu starten, sondern der Download wird fortgesetzt, bis er erfolgreich abgeschlossen ist.

Betroffene Netzwerkpfade

Bei einem LAN-Pfad zwischen dem 9800 und den APs tritt das Problem der Beschädigung des

AP-Images nicht auf, d. h. Pfade mit einer vollständigen IP-MTU von 1500 Byte, geringer Latenz und sehr geringem Paketverlust sind nicht betroffen. Das Problem tritt mit höherer Wahrscheinlichkeit bei CAPWAP-Tunneln über ein WAN auf, die folgenden Pfadmerkmale aufweisen:

- hoher Paketverlust
- niedrige CAPWAP-MTU (kleiner als 1485 Byte) - je niedriger die MTU, desto höher das Risiko
 - Eine niedrige CAPWAP-MTU kann ein Symptom für einen Paketverlust sein.

So erkennen Sie, ob Ihr Netzwerkpfad gefährdet ist

- Überprüfen Sie auf dem 9800 CAPWAP Path MTU mit

```
<#root>
```

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

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

```
MTU
```

```
Mode          McastIf
```

```
-----
```

Mode	McastIf	SourceIP	SrcPort	DestIP	DestPort
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				

```
1485
```

```
multicast Mc1
```


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


```
1005
```

```
multicast Mc1
```

- Wenn die MTU eines bestimmten AP schwankt, ist dies ein guter Risikoindikator
- Oder **allgemeine App-Konfiguration anzeigen | CAPWAP\ Path\ MTU einschließen** (in Show tech-support wireless)
 - Verwenden Sie [Wireless Config Analyzer Express \(WCAE\)](#) auf der Ausgabe des 9800 "show tech-support wireless", um die MTU der Access Points unter Access Points > Configuration (Zugangspunkte > Konfiguration) anzuzeigen.
- Verwenden Sie auf dem 9800 die Option "show ap uptime" (Verfügbarkeit anzeigen), und suchen Sie nach APs mit einer langen "AP Up Time" (Verfügbarkeitszeit des AP) und einer kurzen "Association Up Time" (Verfügbarkeitszeit des AP).
 - Wenn es keinen Grund für eine kurze Aktivierungszeit der APs gibt (d. h. keine Neukonfiguration), kann dies auf einen gefährdeten Netzwerkpfad hinweisen.

Sichere Upgrades von einer nicht fixierten AP-Softwareversion

 Hinweis: Wenn Ihre Bereitstellung anfällig für Image-Beschädigungen ist (d. h. betroffene AP-Modelle, Ausführung von Software ohne Fehlerbehebung für das Boot-a-Bad-Image-

 Syndrom, mit risikobehafteten WAN-Eigenschaften), dann aktualisieren Sie nicht, indem Sie einfach die 9800-Software aktualisieren, und die APs wieder beitreten und die neue Software herunterladen - sie können Image-Beschädigungen unterliegen und einen Boot-Loop eingeben. Verwenden Sie stattdessen eine der folgenden Methoden:

Upgrade mithilfe eines lokalen WLC auf die APs

Wenn möglich, sollte ein Staging-Controller im LAN der APs platziert werden - dies kann ein 9800-CL oder (bei Wave 2 / Wi-Fi 6 APs) ein AP im EWC-Modus sein, und die APs auf die Zielversion aktualisiert werden. Sie können dann sicher in den Produktions-Controller integriert werden.

Upgrade über einen AireOS-Controller

Wenn Sie einen AireOS-Controller mit 8.10.190.0 oder höher haben und Ihre AP-Modelle von AireOS unterstützt werden, verbinden Sie die APs mit diesem Controller. Dadurch werden die APs sicher auf feste Software aufgerüstet, und sie können dann sicher dem Produktions-Controller beitreten.

Upgrade mit Archiv-Download-Software

Richten Sie die Ziel-AP-Images auf einem TFTP-/SFTP-Server aus, auf den die Upgrade-APs zugreifen können. AP-Image-Upgrades über TFTP oder SFTP unterliegen nicht dem Image-Beschädigungsproblem. APs können eine Image-Download-Anforderung von der AP-CLI oder (wenn die APs mit dem Controller verbunden sind) von der Controller-CLI initiieren.

1. Richten Sie einen TFTP- oder SFTP-Server an einem für die APs zugänglichen Ort ein. Beachten Sie, dass die TFTP-Leistung durch Latenz begrenzt wird, sodass die Downloads langsam sind, wenn der TFTP-Server von den APs entfernt ist. Da SFTP TCP verwendet, ist der Durchsatz bei Verwendung eines Pfads mit hoher Latenz wesentlich besser. SFTP kann jedoch nicht vom WLC ausgelöst werden, da ein interaktiver Dialog zur Eingabe von Benutzername und Kennwort erforderlich ist.
2. Legen Sie die gewünschten AP-Images auf einem TFTP- oder SFTP-Server ab. [Siehe Tabelle 4 in der Kompatibilitätsmatrix für](#) die AP-Version 15.3(3)J*, die der gewünschten IOS-XE-Version zugeordnet ist. Laden Sie dann die entsprechenden Lightweight AP Software-Images für die betroffenen AP-Modelle von software.cisco.com herunter.
 1. Beispiel: das AP-Image für 17.9.5 für einen CW9162 [isap1g6b-k9w8-tar.153-3.JPN4.tar](#).
3. So aktualisieren Sie über die AP-CLI: Wenn auf die CLI des Access Points über die Konsole oder SSH zugegriffen werden kann:
 1. Geben Sie den Befehl TFTP oder SFTP ein:

```
archive download-sw /no-reload tftp://<IP-Adresse>/<apimage>
```

Oder

```
archive download-sw /no-reload sftp://<IP-Adresse>/<apimage>
```

```
Benutzername:USER
```

```
Kennwort:XXX
```

Dadurch wird das beschädigte Image mit dem gültigen Image überschrieben.

2. Wenn der Image-Download abgeschlossen ist, führen Sie Folgendes aus:
Test-Capwap-Neustart
 Dadurch wird der CAPWAP-Prozess neu gestartet, sodass der Access Point das neu installierte Image erkennt.
3. Um eine große Anzahl von APs über "archive download-sw" zu aktualisieren, anstatt den Befehl in jedem AP einzeln einzugeben, können Sie eine Skriptmethode verwenden. Siehe unten Upgrade-APs über WLAN-Poller.
4. Wenn die APs mit einem Controller verbunden sind, können Sie die APs über die Controller-CLI aktualisieren (nur TFTP):
 1. In IOS-XE:**ap nameAPNAMEtftp-downgradeip.addr.of.server
 imagename.tar**
 2. In AireOS:**config ap tftp-downgradeip.addr.of.server
 imagename.tarAPNAME**
 1. Obwohl CAPWAP-Downloads von AireOS nicht anfällig für Image-Beschädigungen sind, sollten Sie, wenn Sie vorhaben, Ihre APs von AireOS auf 9800 zu migrieren, zuerst ein AP-Image mit den Fixes für Alt-boot und das Boot a Bad Image-Syndrom (8.10.190.0 oder höher) herunterladen, bevor Sie die APs auf die 980 0.
 3. Überwachen Sie die TFTP- oder SFTP-Serverprotokolle, um sicherzustellen, dass alle Access Points das Image erfolgreich heruntergeladen haben. Wenn der Download abgeschlossen ist, wird jeder Access Point neu geladen und führt das neu heruntergeladene Image aus.

AP-Upgrade über Predownload, Fehlerüberwachung

Laden Sie das Ziel-Image auf den 9800, und verwenden Sie AP Predownload, um das neue Image auf den AP zu übertragen. Gleichzeitig wird auf die Beschädigung des AP-Images überwacht.

Schritt 1: Überprüfen Sie, ob SSH unter den AP-Join-Profilen des C9800 WLC aktiviert ist. Richten Sie einen Syslog-Server im Netzwerk ein. Konfigurieren Sie die IP-Adresse des Syslog-Servers unter "AP Join Profile" für alle Standorte, und legen Sie den Wert für das Protokoll-Trap auf Debug fest. Stellen Sie sicher, dass der Syslog-Server Syslogs vom Access Point empfängt.

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

Schritt 2: Laden Sie das Software-Image auf den C9800 WLC herunter, um das Vorabdownload über die CLI vorzubereiten:

```
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
```

Schritt 3: Führen Sie das AP-Image vor dem Download auf den Cisco C9800 WLCs aus:

```
C9800# ap image predownload
```

Hinweis: Je nach Umfang und Art der Bereitstellung kann dies zwischen einigen Minuten und einigen Stunden dauern. Starten Sie den Controller oder die APs nicht neu, bis Sie die Gültigkeit ihrer Images überprüft haben!

Schritt 4: Überprüfen Sie nach Abschluss des Vorabdownloads für alle Access Points, ob eine der beiden Protokollmeldungen auf dem Syslog-Server vorhanden ist:

- Die Image-Signatur wurde erfolgreich überprüft.

- Fehler bei der Überprüfung der Bildsignatur: -3

Überprüfen Sie auch die Ausgabe des Befehls `show ap image summary`, und suchen Sie nach allen Instanzen von Failed to Download. Wenn der Zähler ungleich null ist, finden Sie die ausgefallenen APs über `show ap image`. | include Fehlgeschlagen.

Vorsicht: Wenn APs die Image-Signatur protokollieren oder wenn APs das Herunterladen nicht durchführen konnten, FAHREN SIE MIT DEM UPGRADE-PROZESS NICHT WEITER. Wenn alle APs die Meldung "Image signing verify success" (Image-Signierung als erfolgreich bestätigt) zeigten, dann haben alle APs das Image korrekt heruntergeladen, und Sie können das 9800-Upgrade sicher fortsetzen.

Schritt 5: Wenn bei einem Access Point ein Verifizierungsfehler aufgetreten ist oder der Download fehlgeschlagen ist, müssen Sie das Image in der Backup-Partition des Access Points mithilfe des folgenden Verfahrens mit einem Archivdownload eines separaten Access Point-Images überschreiben, um eine Bootschleife zu vermeiden.

Wenn nur wenige Access Points ausgefallen sind, können Sie einfach per SSH auf jeden Access Point zugreifen und die folgenden Schritte ausführen.

```
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
```

Hinweis: "test capwap restart" ist erforderlich, damit der CAPWAP-Prozess des Access Points erkennt, dass das Image in der Backup-Partition aktualisiert wurde. Dies führt zu einer kurzen Dienstunterbrechung, da die CAPWAP-Verbindung mit dem 9800 neu gestartet wird. Wenn dies ein betriebliches Problem darstellt, kann dieser Schritt auf ein Wartungsfenster verschoben werden.

APs mithilfe von WLAN Poller aktualisieren

Wenn die Anzahl der APs, die über Archiv-Download-Software aktualisiert werden, groß ist, können Sie einen automatisierten Prozess mit dem [WLAN-Poller](#) verwenden.

Schritt 1a: Installieren Sie den WLAN-Poller auf einem Mac oder einem [Windows-Computer](#).

Schritt 1b: Füllen Sie die Aplist-CSV-Datei mit den entsprechenden fehlerhaften APs aus.

Schritt 1c: Füllen Sie die cmdlist-Datei mit den folgenden Befehlen aus (Sie können nach eigenem Ermessen immer weitere hinzufügen):

```
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
```

Schritt 1d: Führen Sie den WLAN-Poller aus.

Schritt 1e: Wenn die Ausführung abgeschlossen ist, überprüfen Sie die Protokolldateien aller Access Points, um den erfolgreichen Abschluss zu überprüfen.

Schritt 2: Aktivieren Sie das Bild sofort auf dem C9800 WLC, und laden Sie es neu.

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

Schritt 3: Image auf dem C9800 WLC bestätigen. Wenn Sie diesen Schritt überspringen, kehrt WLC zum vorherigen Software-Image zurück.

```
C9800#install commit
```

Häufig gestellte Fragen

Frage: Ich habe vor einigen Tagen ein Predownload durchgeführt, aber meinen Cisco C9800 WLC und die APs noch nicht neu gestartet. Ich habe keine Syslogs, um zu überprüfen, ob das Image beschädigt ist. Wie kann ich überprüfen, ob das Bild beschädigt ist?

A: Aktivieren Sie die Option `show logging on the APs/syslog`. Wenn in der Ausgabe von `show logging` keine Erfolgs- oder Fehlermeldungen angezeigt werden, können Sie den Befehl `"show flash syslogs"` verwenden, um die Syslog-Ausgabe zu filtern, wenn Sie das Vorabdownload durchgeführt haben. Wenn die Meldung `"Image signing verify success"` (Image-Signierung - Erfolgsüberprüfung) angezeigt wird, wissen Sie, dass der Access Point das Image erfolgreich heruntergeladen hat.

F: Meine Bereitstellung erfolgt zentral, wobei sich die Access Points im lokalen Modus befinden. Muss ich weiterhin die im Abschnitt "Problemumgehung/Lösungen" aufgeführten Schritte ausführen?

A: Dieses Problem wurde nur beim Upgrade von Access Points über eine WAN-Verbindung gemeldet. APs im lokalen Modus und über lokale Netzwerke laufen in höchstem Maße unwahrscheinlich auf dieses Problem hinaus. Daher ist es nicht erforderlich, dieses Verfahren für Upgrades zu befolgen, wenn Sie sicher sind, dass zwischen dem Controller und den APs nur ein sehr geringer Paketverlust auftritt.

F: Ich habe neue einsatzbereite APs. Wie kann ich sie bereitstellen, ohne dass dieses Problem auftritt?

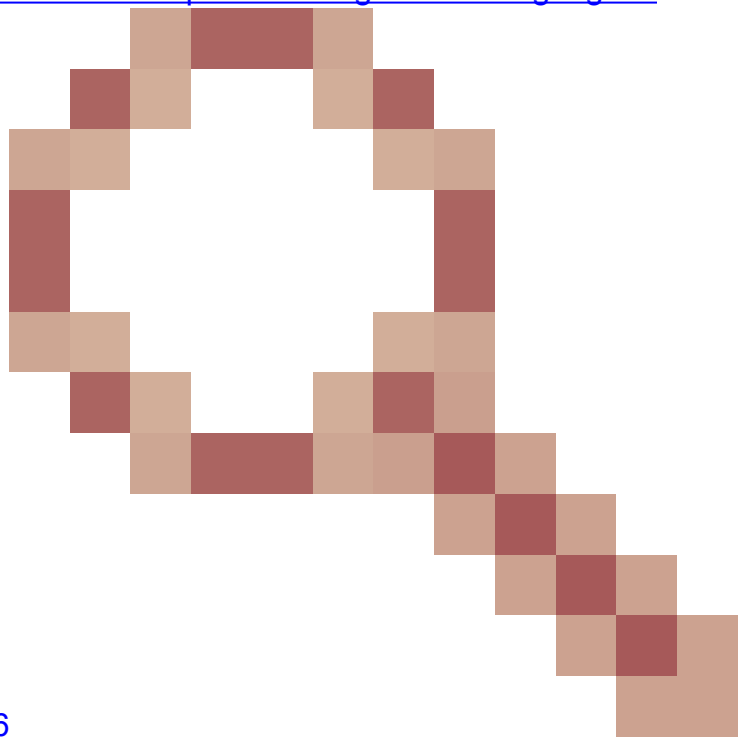
A: Neue, sofort einsatzbereite APs, die Code über WAN herunterladen, sind ebenfalls anfällig für dieses Problem, sofern sie nicht nach Dezember 2023 hergestellt wurden.

F: Was unternimmt Cisco langfristig, um dieses Problem zu beheben, indem CAPWAP-Image-Downloads vom 9800 beschädigt werden?

A: Sobald der Access Point bereits 17.11 oder höher ausgeführt wird, kann er die Out-of-Band-Image-Download-Funktion verwenden, um das Image mithilfe von HTTPS vom Controller abzurufen. TCP überträgt Daten zuverlässig über ein Schiebefenster und ist somit wesentlich schneller über ein WAN als CAPWAP (oder TFTP).

F: Ich habe APs, die sich jetzt in einer Bootschleife befinden. Wie kann ich sie wiederherstellen?

A: Siehe den Artikel [Wiederherstellung von einem Boot-Loop durch Image-Beschädigung auf](#)



[Wave 2 und 11ax Access Points \(CSCvx32806](#)

[\)](#).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.