Validierung und Wiederherstellung von Catalyst APs unter 17.12 aufgrund eines Upgrade-Fehlers

Inhalt

Einleitung

In diesem Dokument wird das Wiederherstellungsverfahren beschrieben, wenn Sie von der Cisco Bug-ID CSCwf25731 betroffen sind. und CSCwf37271

Betroffene Access Points

Diese Access Point-Modelle sind betroffen. Wenn Sie die folgenden Modelle nicht verwenden, sind Sie davon nicht betroffen und es sind keine weiteren Maßnahmen erforderlich:

- Catalyst 9124 (I/D/E)
- Catalyst 9130 (E/A)
- Catalyst 9136I
- Catalyst 9162I
- Catalyst 9163E

- Catalyst 9164I

- Catalyst 9166 (I/D1)
- Catalyst IW9167 (E/A)

Kontext

Upgrades von Systemen, die sich auf 17.12.4/5/6a befanden, auf eine beliebige Version können dazu führen, dass bestimmte Access Point-Modelle unter bestimmten Bedingungen in eine Bootschleife gelangen, was durch einen Fehler bei der Image-Installation aufgrund unzureichenden Speicherplatzes auf dem Zielgerät ausgelöst wird. Dieses Szenario tritt nur während eines Upgrade-Vorgangs mit Access Points auf, z. B. ISSU, vollständige Controller-Image-Installation oder APSP, und hat keine Auswirkungen auf normale Services, den täglichen Betrieb oder SMU-Installationen.

Vor der Durchführung eines Upgrades der möglicherweise betroffenen Access Points sind weitere Schritte erforderlich. Dieses Problem hat keine Problemumgehung und ist nicht von der Konfiguration, dem Bereitstellungstyp oder dem Controller-Modell abhängig.

Dieses Problem betrifft nicht Versionen vor 17.12.4 oder wenn der Access Point eine Version nach 17.12.6a, z. B. 17.15.x, ausführt und keine der betroffenen Versionen installiert hat.

Eine Fehlerbehebung ist für die Cisco IOS XE-Versionen 17.12.4, 17.12.5 und 17.12.6a in Form der jeweiligen APSPs verfügbar. Darüber hinaus ist ein Bereinigungs-APSP für 17.15.4d und 17.18.2 verfügbar, um den verlorenen Speicherplatz für die Bereitstellungen wiederherzustellen, die die betroffene Version verwendet haben und bereits auf eine neuere Version aktualisiert haben.

Wenn Ihr Netzwerk zu einem bestimmten Zeitpunkt von einer der betroffenen Versionen betroffen war oder Sie nicht sicher sind, ob das Netzwerk diese Versionen zuvor verwendet hat, wird empfohlen, die Prüfungen vor einem Upgrade als Vorsichtsmaßnahme durchzuführen.

Details zur Ursache

Access Points der betroffenen Modelle, die die Codes 17.12.4 bis 17.12.6a ausführen, erstellen eine persistente Datei "/storage/cnssdaemon.log", die bis zu 5 MB pro Tag wachsen kann und den gesamten verfügbaren Speicherplatz auf dieser Festplattenpartition nutzen kann. Diese Datei wird beim Neustart nicht gelöscht. Sobald die Partition vollständig verwendet wurde, können Upgrades fehlschlagen, da ein wichtiger Schritt zum Speichern der neuen Dateiversion nicht abgeschlossen ist.

Das Problem wurde durch ein Bibliotheksupdate verursacht, das das Protokollziel für eine interne Komponente geändert hat. Die Protokolldatei wird für den Gerätebetrieb nicht benötigt.

Der Upgrade-Fehler tritt nur auf, wenn der Access Point von Partition 1 ausgeführt wird und der Speicherplatz auf Partition 2 erschöpft ist. Wenn genügend Speicherplatz vorhanden ist oder der Access Point von Partition 2 gestartet wurde, ist das Upgrade erfolgreich

Upgrade-Prüfverfahren

Wenn der WLC aktuell auf17.12.4, 17.12.5, 17.12.6a ist, ist ein Upgrade auf eine Softwareversion mit dem Fix erforderlich, während die folgenden Schritte ausgeführt werden. Bei allen anderen Versionen, die auf dem WLC installiert sind, falls ein Upgrade geplant ist,Es wird dringend empfohlen, diese Anweisungen zu befolgen:

Schritt 1: Überprüfen Sie, ob die Access Points möglicherweise betroffen sind (siehe Tabelle 1). Wenn dies nicht der Fall ist, ist kein Vorabprüfung/Wiederherstellungsprozess erforderlich, und Sie können direkt mit einem Upgrade auf eine der neuesten Versionen fortfahren.

Phase 2: Wenn Sie betroffen sind, führen Sie Vorprüfungen durch, um die Anzahl der betroffenen APs im Abschnitt Vorprüfungen zu ermitteln.

Schritt 3: Führen Sie auf den identifizierten APs die im Abschnitt zur Wiederherstellung beschriebenen Wiederherstellungsschritte aus.

Schritt 4: Führen Sie die Vorabprüfung erneut aus, um sicherzustellen, dass kein anderer Access Point betroffen ist.

Schritt 5: Fahren Sie mit dem Upgrade auf die entsprechenden APSPs oder Softwareversionen fort, die in der Tabelle mit den festen Versionen aufgeführt sind.

Überprüfen Sie anhand dieser Tabelle, ob dieser Hinweis auf Sie zutrifft:

Tabelle 1 - Anwendbarkeit des Upgrade-Pfads

Aktuelle Version	Ziel	Relevanz des Problems	Vor dem Upgrade Precheck erforderlich	Ziel-/Upgrade-Pfad	Upgrade-Vorzeichen	Kommentare
17.3.x/17.6.x/17.9.x	17.12.x	Nein	Nein	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	Nein	Versionshinweise für Ziel überprüfen
17.9.x	Beliebig (mit Ausnahme von 17.12.4/5/6a)	Nein	Nein	Pfad für Ziel-Upgrade folgen	Nein	17.9,1 bis .5 unterstützen kein direktes Upgrade auf 17.15,

						verwenden Sie 17.9.6 oder höher Weitere Informationen finden Sie in den Versionshinweisen.
17.12.1 bis 17.12.3	Beliebig (mit Ausnahme von 17.12.4/5/6a)	Nein	Nein	Pfad für Ziel-Upgrade folgen	Regelmäßiger Prozess	Versionshinweise für Ziel überprüfen
17.12.4/5/6a	17.12.x(4,5,6a usw.), APSP	Ja	Ja	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	Ja	Nach der Installation eines festen APSP sind keine zusätzlichen Vorabprüfungen für zukünftige 17.12-Upgrades erforderlich.
17.12.4/5/6a	17.15.x/17.18.x	Ja	Ja	Führen Sie ein Upgrade auf den jeweiligen APSP 17.12.x durch, und aktualisieren Sie anschließend auf 17.15.x + APSPx oder 17.18.x + APSPx.	Ja für das erste APSP-Upgrade 17.12 und Nein für die nachfolgenden Upgrades.	
Bei allen Versionen war das vorherige Image eines von 17.12.4/5/6a.	17.15.x	Ja	Ja	17.15.x + APSPx	Ja	

Bei allen Versionen war das vorherige Image eines von 17.12.4/5/6a.	17.18.x	Ja	Ja	17.18.x + APSPx	Ja	
Über 17,15 Neue Bereitstellung	Beliebig	Nein	Nein	Beliebig	Nein	
17.18. Neue Bereitstellung	Beliebig	Nein	Nein	Beliebig	Nein	

Anmerkung: Wenn das Netzwerk nicht läuft und in der Vergangenheit nicht ausgeführt wurde (17.12.4, 17.12.5, 17.12.6a), ist das Problem nicht anwendbar.

Anmerkung: Alle anderen Versionen, die nicht explizit in der Spalte "Aktuell" aufgeführt sind, folgen dem empfohlenen Upgrade-Pfad.

Feste Versionen

Controller	AP-Image-Version
17.12.4 + APSP13	17.12.4.213
17.12.5 + APSP9	17.12.5.209
17.12.6a + APSP1	17.12.6.201
17.15.3 + APSP12	17.15.3.212
17.15.4b + APSP6	17.15.4.206
17.15.4d + APSP1	17.15.4.225
17.18.1 + APSP3	17.18.1.203

17.18.2 + APSP1	17.18.2.201

Vorabprüfungen

Führen Sie die aktuellen Schritte aus, um zu evaluieren, ob das Netzwerk für dieses Problem anfällig ist. Diese Schritte bieten einen Überblick. Verwenden Sie jedoch zur tatsächlichen Erkennung von APs den Abschnitt "Precheck-Skripte", um diesen Prozess zu automatisieren:

- Bestätigen Sie, ob es sich bei den Access Point-Images um eines handelt, falls die betroffenen Versionen vorhanden sind, unter den Spalten für das primäre oder das Backup-Image:

```
9800-l#show ap image
Total number of APs  : 4

Number of APs
        Initiated                 : 0
        Downloading               : 0
        Predownloading            : 0
        Completed downloading     : 0
        Completed predownloading  : 0
        Not Supported             : 0
        Failed to Predownload     : 0
        Predownload in progress   : No

AP Name             Primary Image          Backup Image            Predownload Status   Predownload Ver
-------------------------------------------------------------------------------------------------------
Ap1                 17.12.5.41        17.12.4.201               None                 0.0.0.0
Ap2                 17.12.5.41        17.12.4.201               None                 0.0.0.0
Ap3                 17.12.5.41        17.12.4.201               None                 0.0.0.0
Ap4                 17.12.5.41        17.12.4.201               None                 0.0.0.0
```

- Eine ähnliche Überprüfung kann im Access Point durchgeführt werden:

```
AP# show version
AP Running Image     : 17.12.5.41
Primary Boot Image   : 17.12.5.41
Backup Boot Image    : 17.12.5.209
Primary Boot Image Hash: 93ef1e703a5e7c5a4f97b8f59b220f52d94dd17c527868582c0048caad6397a9f3526c644f94a5
Backup Boot Image Hash: 4bbe4a0d9edc3cad938a7de399d3c2e08634643a2623bae65973ef00deb154b8eb7c7917eeecdd4
1 Multigigabit Ethernet interfaces

Any Boot Image is one of the following:
- 17.12.4.0 to 17.12.4.212
- 17.12.5.0 to 17.12.5.208
- 17.12.6.0 to 17.12.6.200
```

- Aktuelle Startpartition überprüfen:

```
AP# show boot
--- Boot Variable Table ---
BOOT path-list: part1
Console Baudrate: 9600 Enable Break:

The “BOOT path-list:” should be part1, suggesting that the Backup partition is running on part2.
```

- Aktuelle Dateisystemnutzung überprüfen:

```
AP# show filesystems
Filesystem                Size      Used Available Use% Mounted on
devtmpfs                880.9M         0    880.9M   0% /dev
/sysroot                883.8M    219.6M    664.1M  25% /
tmpfs                     1.0M     56.0K    968.0K   5% /dev/shm
tmpfs                   883.8M         0    883.8M   0% /run
tmpfs                   883.8M         0    883.8M   0% /sys/fs/cgroup
/dev/ubivol/part1       372.1M     79.7M    292.4M  21% /part1
/dev/ubivol/part2       520.1M    291.3M    228.9M  56% /part2

The “Use%” for “/dev/ubivol/part2” is close to 100%.
```

- Überprüfen Sie die Image-Integrität für beide Partitionen:

```
AP# show image integrity
/part1(Backup) 17.12.5.209
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good
/part2(primary) 17.12.5.41
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good

The image integrity should be “Good” for all fields in both the partitions. If not Good open a TAC case
```

Im nächsten Abschnitt führen wir Sie durch die Skripte, die den Vorabprüfungsprozess für alle APs automatisieren.

Precheck-Skript

WLAN Poller(kann hier heruntergeladen werden)

Schritt 1: Extrahieren Sie den WLAN-Abfrageprozess an den gewünschten Dateispeicherort.

Phase 2: Ändern Sie diese Werte in der Datei "config.ini":

```
wlc_type: 2
mode: ssh
ap_mode: ssh

; set global WLC credentials
wlc_user: username
wlc_pasw: password
wlc_enable: enable_password

; set global AP credentials
ap_user: ap_username
ap_pasw: ap_password
ap_enable: ap_enable_password

[WLC-1]
active: True
ipaddr:


mode: ssh
```

Schritt 3: Kommentieren Sie den Rest des Standardinhalts und die folgende Liste von Befehlen in die Dateien "cmdlist_cos" und "cmdlist_cos_qca".

```
show clock
show version
show flash
show flash | i cnssdaemon.log
show boot
show filesystems
show image integrity
```

Beispiel unten:

```
# snippet to download the Debug image on COS APs
# show version | in Compiled
# archive download-sw /reload tftp://


        /


#
show clock
show version
show flash
show flash | i cnssdaemon.log
show boot
show filesystems
```

```
show image integrity
```

Schritt 4: Führen Sie den Wlanpoller mit ".\wlanpoller.exe" aus. Der WLAN-Abfrageprozess wird per SSH mit allen APs ausgeführt, und die Ausgaben für alle APs werden abgerufen.

Schritt 5: Nach der Ausführung wird ein "Daten"-Ordner erstellt. Geben Sie den Ordner ein und gehen Sie bis zum Ende, wo Sie mehrere Dateien für jeden der APs erstellt haben.

Schritt 6: Kopieren Sie den separat bereitgestellten "ap_detection_script.py" in diesen Ordner und führen Sie ihn aus. Das Skript finden Sie unter dem folgenden Box-Link:

https://pubhub.devnetcloud.com/media/wireless-troubleshooting-tools/docs/9800-scripts/ap_detection_script.zip

Dadurch wird im selben Ordner eine Datei mit dem Namen "Status_check_results.log" erstellt. Diese enthält die Liste der Access Points, die sich möglicherweise in einem problematischen Zustand befinden und einige Wiederherstellungs-/zusätzliche Schritte erfordern, bevor Sie mit dem Upgrade fortfahren können.

Wiederherstellungsprozess:

Ausgehend vom aktuellen Zustand jedes als problematisch eingestuften Access Points würde das Skript außerdem Hinweise dazu liefern, wie diese Access Points am besten wiederhergestellt werden können. Im Folgenden sind die detaillierten Schritte aufgeführt, die Sie für die einzelnen Optionen durchführen müssen.

Option 1: Partitionsswap

Schritt 1: Stellen Sie sicher, dass der Access Point nicht mit dem Controller kommuniziert, damit der Access Point nicht auf seine vorherige Partition/Version zurückgesetzt wird. Dies kann durch eine Zugriffsliste auf dem Controller-Gateway erreicht werden.

Phase 2: Konfigurieren Sie von den potenziell betroffenen Access Points den Start für Partition 2:

```
AP# config boot path 2
```

Schritt 3: Starten Sie den Access Point neu, damit er mit dem Image auf Partition 2 bootet:

```
AP# reset
```

Schritt 4: Lassen Sie den Access Point dem Controller beitreten, nachdem das Upgrade auf dem

Controller abgeschlossen ist. Der Access Point wird hinzugefügt und das neue Image heruntergeladen.

HINWEIS: Wenn Sie diese Option aus irgendeinem Grund nicht in Betracht ziehen, können Sie jederzeit ein TAC-Ticket erstellen und mit Option 2 auch für diese APs fortfahren.

Option 2: Öffnen Sie ein TAC-Ticket, damit das TAC den Access Point von der Root-Shell bereinigt (führen Sie nach diesem Prozess das normale Upgrade durch).

Option 3: Abgesicherter Zustand, aber Access Point verfügt über fehlerhaftes Image in der Backup-Partition

Die APs enden in diesem Zustand, meist nachdem das Upgrade auf eine feste Version abgeschlossen wurde. Dieser Zustand deutet darauf hin, dass der Access Point eine feste Version ausführt, die Backup-Version jedoch noch fehlerhaft ist. Um Fehler zu vermeiden, empfehlen wir, die Sicherung der Access Points durch ein gutes Image zu ersetzen, d. h. durch eine Version, in der dieses Problem nicht auftritt. Je nach Anzahl der betroffenen APs können Sie entweder ein Bild archivieren oder es einfach vorher herunterladen, ohne es zu aktivieren.

Option 4: Die Prüfung der Bildintegrität für diese APs ist fehlgeschlagen.

Öffnen Sie ein TAC-Ticket, damit der TAC-Techniker diese APs korrigieren kann, bevor Sie mit dem Upgrade fortfahren.

Option 5: Die Prüfung der Bildintegrität für diese APs ist fehlgeschlagen.

Die aktuelle Partition ist nicht anfällig, aber der Flash-Speicher ist niedrig. Es wird empfohlen, ein TAC zu öffnen, um cnssdaemon.log über devshell vom Speicher zu bereinigen.

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.