Validate and Recover Catalyst APs on 17.12 Impacted by Upgrade Failure

Contents

Introduction

This document describes the recovery procedure when you are affected by Cisco bug ID CSCwf25731 and CSCwf37271

Affected Access Points

These Access Point models are impacted. if you are not using the below models you are not impacted and not further actions are required:

- Catalyst 9124 (I/D/E)
- Catalyst 9130 (I/E)
- Catalyst 9136I
- Catalyst 9162I
- Catalyst 9163E
- Catalyst 9164I
- Catalyst 9166 (I/D1)
- Catalyst IW9167 (I/E)

Context

Upgrades from systems that have been on 17.12.4/5/6a to any release can cause specific Access Points models to enter a boot loop under certain conditions, triggered by image install failure due to insufficient disk space on the target device storage. This scenario only occurs during an upgrade operation involving Access Points, for example ISSU, full controller image install or APSP, and it does not impact any normal service, day to day operations, or SMU installs.

Additional steps are required before performing any upgrade on the possibly impacted Access Points. This issue has no workaround, and it is not dependent on configuration, deployment type or controller model

This issue does not impact versions prior to 17.12.4, or if the Access Point is running any release after 17.12.6a, for example 17.15.x and it has never installed any of the impacted versions.

A fix is available for Cisco IOS XE releases 17.12.4, 17.12.5, 17.12.6a, in the form of respective APSPs. Additionally, a cleanup APSP is available for 17.15.4d and 17.18.2, to recover the lost space, for those deployments that were using the impacted release, and have already upgraded to a later version.

If your network has been on any of the impacted releases at some point or if you are not sure if the network has used those versions previously, it is recommended to perform the checks before any upgrade as a precaution

Root Cause Details

Access points of the affected models, running codes 17.12.4 to 17.12.6a, create a persistent file "/storage/cnssdaemon.log", that can grow up to 5 MB per day, and use all the available space on that disk partition. This file is not cleared on reboot. Once the partition is fully used, upgrades can fail, as a critical step on storing the new file version is not completed.

The issue was introduced by a library update, that modified the log destination for an internal component. The log file is not needed for device operation

The upgrade failure only happens if the AP is running from partition 1, and the partition 2 space has been exhausted. If there is enough space, or AP has booted from partition 2, the upgrade is successful

Upgrade Check Procedure

Ifthe WLC is currently on17.12.4, 17.12.5, 17.12.6a, upgrade is mandatory to a software version with the fix while following the below steps. For any other versions installed on the WLC, if planning to upgrade,it is highly recommended tofollow these instructions:

Step 1: Check if the Access Points are potentially impacted (Refer to Table 1). If not impacted, no Pre-check/Recovery process is required, and you can proceed directly to upgrade to any of the latest releases.

Step 2: If you are impacted, perform prechecks to identify the number of APs affected in the Prechecks section.

Step 3: On the identified APs, perform the recovery steps outlined in the recovery section.

Step 4: Rerun the precheck to confirm that no other AP is affected.

Step 5: Proceed to upgrade to the respective APSPs or software versions mentioned in the Fixed Versions Table.

Please refer this table to verify if this notice is applicable to you:

Table 1 - Upgrade path applicability

Currentversion	**Target**	**Issue Applicability**	**Before upgrade Precheck needed**	**Target/Upgrade Path**	**Upgrade Precheck**	**Comments**
17.3.x / 17.6.x / 17.9 x	17.12.x	No	No	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	No	Check destination Release Notes
17.9.x	Any (Except 17.12.4/5/6a)	No	No	Follow destination upgrade path	No	17.9,1 to .5 do not support direct upgrade to 17.15, use 17.9.6 or higher For more information check release notes
17.12.1 to 17.12.3	Any (Except 17.12.4/5/6a)	No	No	Follow destination upgrade path	Regular Process	Check destination Release Notes
17.12.4/5/6a	17.12.x(4,5,6a etc), APSP	Yes	Yes	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	Yes	After installing a fixed APSP, no additional prechecks are needed for future 17.12 upgrades
17.12.4/5/6a	17.15.x / 17.18.x	Yes	Yes	Upgrade respective 17.12.x APSP then upgrade to 17.15.x + APSPx or 17.18.x + APSPx	Yes for the first 17.12 APSP upgrade and No for the subsequent upgrades.	

Any release, previous image was one of 17.12.4/5/6a	17.15.x	Yes	Yes	17.15.x + APSPx	Yes	
Any release, previous image was one of 17.12.4/5/6a	17.18.x	Yes	Yes	17.18.x + APSPx	Yes	
17.15+ New deployment	Any	No	No	Any	No	
17.18. New deployment	Any	No	No	Any	No	

Note: In general, if the network is not running and has not run 17.12.4, 17.12.5, 17.12.6a in the past, the issue is not applicable

Note: Any other release not explicitly mentioned in the “Current” column follow the recommended upgrade path.

Fixed Releases

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

Pre-Checks

To evaluate if the network is susceptible to this issue, perform the current steps. These steps help provide an overview, but for actual detection of APs please use the section "Precheck scripts" to automate this process:

- Confirm if access point images are one if the impacted releases, under Primary or Backup image columns:

```
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
```

- A similar verification can be performed in the AP:

```
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
```

- Verify current booting partition:

```
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.

- Verify current filesystem usage:

```
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%.

- Verify image integrity for both partitions:

```
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

In the Next Section we walk you through the scripts which automate the precheck process for all the APs.

Precheck script

WLAN Poller(Can be downloaded from here)

Step 1: Extract the WLAN Poller to the desired file location

Step 2: Modify these values in the “config.ini” file:

```
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: <Controller_management_ip_address>
mode: ssh
```

Step 3: Comment the rest of the default contents and the below list of commands to the files “cmdlist_cos” and “cmdlist_cos_qca”.

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

Sample below:

```
# snippet to download the Debug image on COS APs
# show version | in Compiled
# archive download-sw /reload tftp://<tftp server ip-address>/<TAR filename>
#
show clock
show version
show flash
show flash | i cnssdaemon.log
show boot
show filesystems
show image integrity
```

Step 4: Execute the wlanpoller using “.\wlanpoller.exe”. The WLAN poller runs, SSH to all the APs, and get the outputs from these commands for all of them.

Step 5: Post execution, a “data” folder gets created. Enter the folder and go all the way till the end where you have multiple files created for each of the APs.

Step 6: Copy/paste the separately provided “ap_detection_script.py” in this folder and execute it. You can find the script at the below Box link:

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

This creates a file in the same folder by the name “Status_check_results.log”. This has the list of APs which could be potentially in a problematic state and would need some recovery/extra steps before you proceed with your upgrade.

Recovery Process:

Based on the current state of each Access Point which is determined to be problematic, the script would further provide guidance on what would be the most optimized way to recover these APs. Here are the detailed steps that you would need to take for each of the options.

Option 1: Partition Swap

Step 1: Ensure that the AP does not have communication to the controller to avoid the AP reverting to its previous partition/version. This can be achieved through an access-list on the controller gateway.

Step 2: From the potentially impacted APs, configure boot for partition 2:

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

Step 3: Reboot the AP to make it boot with the image on partition 2:

```
AP# reset
```

Step 4: Have the AP join the controller after the upgrade is complete on the controller. The AP joins and download the new image.

NOTE: If you this option is not viable for any reason, you can always open a TAC case and proceed with Option 2 for this set of APs as well.

Option 2: Open a TAC case to have TAC cleanup the AP from root shell (After this process you go ahead with the normal upgrade)

Option 3: Safe state but AP has buggy image in the backup partition

The APs end up in this state mostly after the upgrade to a fixed version has been completed. This state suggests that the AP is running a fixed version but the backup version is still buggy. To err on the side of caution we would reccomend to replace the APs backup with a good image as well i.e a version where this issue is not seen. Depending on the number of APs in question, either archive download an image to the AP or just do a pre download without actually activating it.

Option 4: Image integrity check has failed for these APs

Open a TAC case to have TAC engineer rectify these APs before proceeding with the upgrade.

Option 5: Image integrity check has failed for these APs

Current Partition is not susceptible but the flash storage is low. Reccomend to open a TAC to clean up the cnssdaemon.log from the storage via the devshell.