업그레이드 실패의 영향을 받는 17.12의 Catalyst AP 검증 및 복구

목차

소개

이 문서에서는 Cisco 버그 ID CSCwf의 영향을 받는 경우의 복구 절차에 대해 설명합니다25731 및 CSCwf37271

영향을 받는 액세스 포인트

이러한 액세스 포인트 모델은 영향을 받습니다. 아래 모델을 사용하지 않는 경우 영향을 받지 않으며 추가 작업이 필요하지 않습니다.

- 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)

컨텍스트

17.12.4/5/6a에 있는 시스템에서 모든 릴리스로 업그레이드하면 특정 액세스 포인트 모델이 특정 조건에서 부팅 루프에 들어갈 수 있으며, 이는 대상 장치 스토리지의 디스크 공간 부족으로 인한 이미지 설치 실패로 트리거됩니다. 이 시나리오는 액세스 포인트(예: ISSU, 전체 컨트롤러 이미지 설치 또는 APSP)와 관련된 업그레이드 작업 중에만 발생하며, 정상적인 서비스, 일상적인 작업 또는 SMU 설치에 영향을 미치지 않습니다.

영향을 받을 가능성이 있는 액세스 포인트에 대한 업그레이드를 수행하기 전에 추가 단계가 필요합니다. 이 문제는 해결 방법이 없으며 컨피그레이션, 구축 유형 또는 컨트롤러 모델에 종속되지 않습니다

이 문제는 17.12.4 이전 버전이나 액세스 포인트가 17.12.6a 이후 릴리스(예: 17.15.x)를 실행 중이고 영향을 받은 버전을 설치한 적이 없는 경우에는 영향을 받지 않습니다.

각 APSP의 형태로 Cisco IOS XE 릴리스 17.12.4, 17.12.5, 17.12.6a에 대한 수정 사항이 제공됩니다. 또한, 영향을 받는 릴리스를 사용하고 있고 이미 최신 버전으로 업그레이드된 구축의 경우 17.15.4d 및 17.18.2에서 정리 APSP를 사용하여 손실된 공간을 복구할 수 있습니다.

네트워크가 어떤 시점에 영향을 받는 릴리스에 포함되어 있거나, 네트워크가 해당 버전을 이전에 사용했는지 확실하지 않은 경우, 사전 예방 차원에서 업그레이드 전에 검사를 수행하는 것이 좋습니다

근본 원인 세부 정보

코드 17.12.4~17.12.6a를 실행하는 해당 모델의 액세스 포인트는 매일 5MB까지 확장 가능한 영구 파일 "/storage/cnssdaemon.log"을 만들고 해당 디스크 파티션의 사용 가능한 모든 공간을 사용합니다. 재부팅 시 이 파일은 지워지지 않습니다. 파티션을 완전히 사용하면 업그레이드가 실패할 수 있습니다. 새 파일 버전을 저장하는 중요한 단계가 완료되지 않기 때문입니다.

내부 구성 요소의 로그 대상을 수정한 라이브러리 업데이트에 의해 문제가 발생했습니다. 로그 파일은 디바이스 작업에 필요하지 않습니다

업그레이드 실패는 AP가 파티션 1에서 실행 중이고 파티션 2 공간이 모두 소진된 경우에만 발생합니다. 공간이 충분하거나 AP가 파티션 2에서 부팅된 경우 업그레이드에 성공합니다

업그레이드 확인 절차

WLC가 현재 17.12.4, 17.12.5, 17.12.6a에 있는 경우, 아래 단계에 따라 소프트웨어 버전으로 업그레이드해야 합니다. WLC에 설치된 다른 버전의 경우, 업그레이드할 계획이면,다음 지침을 따르는 것이 좋습니다.

1단계: 액세스 포인트가 잠재적으로 영향을 받는지 확인합니다(표 1 참조). 영향을 받지 않는 경우 사전 확인/복구 프로세스가 필요하지 않으며, 최신 릴리스로 곧바로 업그레이드할 수 있습니다.

2단계: 영향을 받는 경우 사전 검사를 수행하여 Prechecks 섹션에서 영향을 받는 AP의 수를 확인합니다.

3단계: 식별된 AP에서 복구 섹션에 설명된 복구 단계를 수행합니다.

4단계: 다른 AP가 영향을 받지 않는지 확인하려면 사전 검사를 다시 실행하십시오.

5단계: Fixed Versions(고정 버전) 표에 나와 있는 해당 APSP 또는 소프트웨어 버전으로 업그레이드하십시오.

이 표가 귀하에게 적용되는지 확인하십시오.

표 1 - 업그레이드 경로 적용 가능성

현재 버전	대상	문제 적용 가능성	업그레이드 전 사전 확인 필요	대상/업그레이드 경로	업그레이드 사전 확인	의견
17.3.x/17.6.x/17.9 x	17.12.x	아니요	아니요	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	아니요	대상 릴리스 정보 확인
17.9.x	모두 (17.12.4/5/6a 제외)	아니요	아니요	대상 업그레이드 경로 팔로우	아니요	17.9,1에서 .5로 업그레이드하는 경우 17.15로 직접 업그레이드할 수 없으며 17.9.6 이상 사용 자세한 내용은 릴리스 정보를 참조하십시오.
17.12.1~17.12.3	모두 (17.12.4/5/6a 제외)	아니요	아니요	대상 업그레이드 경로 팔로우	일반 프로세스	대상 릴리스 정보 확인

17.12.4/5/6a	17.12.x(4,5,6a 등), APSP	예	예	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	예	고정 APSP를 설치한 후 향후 17.12 업그레이드를 위해 추가 사전 점검이 필요하지 않습니다
17.12.4/5/6a	17.15.x / 17.18.x	예	예	각 17.12.x APSP를 업그레이드한 다음 17.15.x + APSPx 또는 17.18.x + APSPx로 업그레이드합니다.	첫 17.12 APSP 업그레이드의 경우 예, 이후 업그레이드의 경우 아니요.	
모든 릴리스에서 이전 이미지는 17.12.4/5/6a 중 하나였습니다.	17.15.x	예	예	17.15.x + APSPx	예	
모든 릴리스에서 이전 이미지는 17.12.4/5/6a 중 하나였습니다.	17.18.x	예	예	17.18.x + APSPx	예	
17.15 이상 새 구축	모두	아니요	아니요	모두	아니요	
17.18 . 새 구축	모두	아니요	아니요	모두	아니요	

참고: 일반적으로 네트워크가 실행되고 있지 않고 과거에 17.12.4, 17.12.5, 17.12.6a를 실행하지 않은 경우에는 이 문제를 적용할 수 없습니다

참고: "현재" 열에 명시적으로 언급되지 않은 다른 릴리스는 권장 업그레이드 경로를 따릅니다.

고정 릴리스

컨트롤러	AP 이미지 버전
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

사전 확인

네트워크에 이 문제가 발생할 가능성이 있는지 평가하려면 현재 단계를 수행하십시오. 이 단계에서는 개요를 제공하는 데 도움이 되지만 AP를 실제로 탐지하려면 "스크립트 사전 검사" 섹션을 사용하여 이 프로세스를 자동화하십시오.

- Primary 또는 Backup image(기본 또는 백업 이미지) 열에서 액세스 포인트 이미지가 영향을 받는 릴리스인지 확인합니다.

```
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
```

- AP에서도 유사한 검증을 수행할 수 있습니다.

```
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
```

- 현재 부팅 파티션 확인:

```
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.
```

- 현재 파일 시스템 사용 확인:

```
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%.
```

- 두 파티션에 대한 이미지 무결성을 확인합니다.

```
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
```

다음 섹션에서는 모든 AP에 대한 사전 검사 프로세스를 자동화하는 스크립트를 살펴봅니다.

사전 검사 스크립트

WLAN Poller(여기서 다운로드 가능)

1단계: 원하는 파일 위치로 WLAN 폴러 추출

2단계: "config.ini" 파일에서 다음 값을 수정합니다.

```
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
```

3단계: 기본 내용의 나머지 부분과 명령의 아래 목록을 "cmdlist_cos" 및 "cmdlist_cos_qca" 파일에 주석 처리합니다.

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

아래 예제:

```
# 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
```

4단계: ".\wlanpoller.exe"를 사용하여 wlanpoller를 실행합니다. WLAN 폴러가 실행되고 모든 AP에 SSH가 적용되며 모든 AP에 대해 이 명령에서 출력을 가져옵니다.

5단계: 실행 후 "데이터" 폴더가 생성됩니다. 폴더를 입력하고 각 AP에 대해 여러 파일이 생성된 끝까지 이동합니다.

6단계: 별도로 제공된 "ap_detection_script.py"를 이 폴더에 복사/붙여넣고 실행합니다. 아래 상자 링크에서 스크립트를 찾을 수 있습니다.

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

이렇게 하면 "Status_check_results.log"라는 이름의 파일이 동일한 폴더에 생성됩니다. 여기에는 문제가 발생할 수 있는 AP 목록이 있으며 업그레이드를 진행하기 전에 복구/추가 단계가 필요합니다.

복구 프로세스:

문제가 있는 것으로 확인된 각 액세스 포인트의 현재 상태에 따라 스크립트는 이러한 AP를 복구하는 가장 최적화된 방법이 무엇인지에 대한 지침을 추가로 제공합니다. 각 옵션에 대해 수행해야 할 자세한 단계는 다음과 같습니다.

옵션 1: 파티션 스왑

1단계: AP가 이전 파티션/버전으로 되돌아가는 것을 방지하기 위해 AP가 컨트롤러와 통신하지 않는지 확인합니다. 이는 컨트롤러 게이트웨이의 액세스 목록을 통해 달성할 수 있습니다.

2단계: 영향을 받을 가능성이 있는 AP에서 파티션 2에 대한 부팅을 구성합니다.

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

3단계: AP를 재부팅하여 파티션 2의 이미지로 부팅합니다.

```
AP# reset
```

4단계: 컨트롤러에서 업그레이드가 완료된 후 AP가 컨트롤러에 조인하도록 합니다. AP가 조인하고 새 이미지를 다운로드합니다.

참고: 어떤 이유로든 이 옵션을 사용할 수 없는 경우, 항상 TAC 케이스를 열고 이 AP 세트에 대해서도 옵션 2를 계속 사용할 수 있습니다.

옵션 2: TAC 케이스를 열어 TAC에서 루트 셸에서 AP를 정리하도록 합니다(이 프로세스 이후에는 일반 업그레이드를 진행합니다).

옵션 3: 안전한 상태이지만 AP에 백업 파티션에 버기 이미지가 있음

AP는 대부분 고정 버전으로의 업그레이드가 완료된 후에 이 상태가 됩니다. 이 상태는 AP가 고정 버전을 실행 중이지만 백업 버전이 여전히 버그가 있음을 나타냅니다. 주의해야 할 경우 AP 백업을 좋은 이미지, 즉 이 문제가 보이지 않는 버전으로 교체하는 것이 좋습니다. 문제가 되는 AP의 수에 따라, 아카이브는 이미지를 AP에 다운로드하거나 실제로 활성화하지 않고 사전 다운로드만 수행합니다.

옵션 4: 이 AP에 대한 이미지 무결성 검사에 실패했습니다.

업그레이드를 진행하기 전에 TAC 엔지니어가 이러한 AP를 수정하도록 하려면 TAC 케이스를 여십시오.

옵션 5: 이 AP에 대한 이미지 무결성 검사에 실패했습니다.

현재 파티션은 영향을 받지 않지만 플래시 스토리지가 부족합니다. TAC를 열어 devshell을 통해 저장소에서 cnssdaemon.log를 정리하는 것이 좋습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.