Validar y recuperar los puntos de acceso Catalyst en 17.12 afectados por un fallo de actualización

Contenido

Introducción

Este documento describe el procedimiento de recuperación cuando se ve afectado por el ID de bug de Cisco CSCwf25731 y CSCwf37271

Puntos de acceso afectados

Estos modelos de punto de acceso se ven afectados. si no está utilizando los siguientes modelos, no se verá afectado y no se requerirán más acciones:

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

- Catalyst 9164I

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

Contexto

Las actualizaciones de sistemas que han estado en 17.12.4/5/6a a cualquier versión pueden hacer que modelos de puntos de acceso específicos entren en un bucle de arranque en ciertas condiciones, desencadenadas por un error en la instalación de la imagen debido a un espacio de disco insuficiente en el almacenamiento del dispositivo de destino. Este escenario solo ocurre durante una operación de actualización que involucra puntos de acceso, por ejemplo ISSU, instalación completa de la imagen del controlador o APSP, y no afecta a ningún servicio normal, operaciones diarias o instalaciones de SMU.

Se requieren pasos adicionales antes de realizar cualquier actualización en los puntos de acceso que puedan verse afectados. Este problema no tiene solución alternativa y no depende de la configuración, el tipo de implementación o el modelo de controlador

Este problema no afecta a las versiones anteriores a 17.12.4, o si el punto de acceso está ejecutando cualquier versión posterior a 17.12.6a, por ejemplo 17.15.x y nunca ha instalado ninguna de las versiones afectadas.

Hay una corrección disponible para las versiones 17.12.4, 17.12.5, 17.12.6a de Cisco IOS XE, en forma de los respectivos APSP. Además, una limpieza APSP está disponible para 17.15.4d y 17.18.2, para recuperar el espacio perdido, para aquellas implementaciones que estaban utilizando la versión afectada, y ya han actualizado a una versión posterior.

Si su red ha estado en cualquiera de las versiones afectadas en algún momento o si no está seguro de si la red ha utilizado esas versiones anteriormente, se recomienda realizar las comprobaciones antes de cualquier actualización como precaución

Detalles de la causa raíz

Los puntos de acceso de los modelos afectados, que ejecutan los códigos 17.12.4 a 17.12.6a, crean un archivo persistente "/storage/cnssdaemon.log", que puede crecer hasta 5 MB al día, y utilizan todo el espacio disponible en esa partición de disco. Este archivo no se borra al reiniciar. Una vez que la partición se ha utilizado completamente, las actualizaciones pueden fallar, ya que un paso crítico en el almacenamiento de la nueva versión del archivo no se ha completado.

El problema fue introducido por una actualización de la biblioteca, que modificó el destino del registro para un componente interno. El archivo de registro no es necesario para el funcionamiento del dispositivo

La falla de actualización solo ocurre si el AP se está ejecutando desde la partición 1 y el espacio de la partición 2 se ha agotado. Si hay suficiente espacio, o el AP se ha iniciado desde la partición 2, la actualización es exitosa

Procedimiento de comprobación de actualización

Si el WLC está actualmente en17.12.4, 17.12.5, 17.12.6a, la actualización es obligatoria a una versión de software con la corrección mientras que sigue los pasos siguientes. Para cualquier otra versión instalada en el WLC, si planea actualizar,se recomienda encarecidamente seguir estas instrucciones:

Paso 1: Compruebe si los puntos de acceso están potencialmente afectados (consulte la tabla 1). Si no se ve afectado, no se requiere ningún proceso de comprobación previa/recuperación y puede continuar directamente con la actualización a cualquiera de las versiones más recientes.

Paso 2: Si se ve afectado, realice comprobaciones previas para identificar el número de AP afectados en la sección Comprobaciones previas.

Paso 3: En los AP identificados, realice los pasos de recuperación descritos en la sección de recuperación.

Paso 4: Vuelva a ejecutar la comprobación previa para confirmar que no hay otro AP afectado.

Paso 5: Continúe actualizando a las respectivas versiones de APSP o software mencionadas en la Tabla de Versiones Fijas.

Consulte esta tabla para comprobar si este aviso es aplicable a su caso:

Tabla 1: Aplicabilidad de la ruta de actualización

Versión Actual	Objetivo	Aplicabilidad del problema	Antes de actualizar Se necesita comprobación previa	Ruta de destino/actualización	Comprobación previa de actualización	Comentar
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	Comproba notas de l versión de destino
17.9.x	Cualquiera (Excepto 17.12.4/5/6a)	No	No	Seguir ruta de actualización de destino	No	17.9,1 a .5 admiten la actualizac directa a 1 utilice 17.9 superior

						Para obte más informació consulte la notas de la versión
17.12.1 a 17.12.3	Cualquiera (Excepto 17.12.4/5/6a)	No	No	Seguir ruta de actualización de destino	Proceso normal	Comproba notas de la versión de destino
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	Después d instalar un APSP fijo, necesitan comproba previas adicionale futuras actualizac 17.12
17.12.4/5/6a	17.15.x / 17.18.x	Yes	Yes	Actualice las respectivas 17.12.x APSP y, a continuación, actualice a 17.15.x + APSPx o 17.18.x + APSPx	Sí para la primera actualización de APSP 17.12 y No para las actualizaciones posteriores.	
Cualquier versión, la imagen anterior era una de 17.12.4/5/6a	17.15.x	Yes	Yes	17.15.x + APSPx	Yes	
Cualquier versión, la imagen anterior era una de 17.12.4/5/6a	17.18.x	Yes	Yes	17.18.x + APSPx	Yes	

+ de 17,15 Nueva implementación	cualquiera	No	No	cualquiera	No	
17.18. Nueva implementación	cualquiera	No	No	cualquiera	No	

Nota: En general, si la red no se está ejecutando y no ha ejecutado 17.12.4, 17.12.5, 17.12.6a en el pasado, el problema no es aplicable

Nota: Cualquier otra versión no mencionada explícitamente en la columna "Current" sigue la ruta de actualización recomendada.

Versiones Corregidas

Controlador	Versión de imagen AP
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

Comprobaciones previas

Para evaluar si la red es susceptible a este problema, siga los pasos actuales. Estos pasos ayudan a proporcionar una descripción general, pero para la detección real de los AP, utilice la sección "Scripts de comprobación previa" para automatizar este proceso:

- Confirme si las imágenes del punto de acceso son una si las versiones afectadas, en Columnas de imagen principal o de copia de seguridad:

```
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
```

- Se puede realizar una verificación similar en el 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
```

- Verificar la partición de arranque actual:

```
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.
```

- Verificar el uso actual del sistema de archivos:

```
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%.
```

- Verifique la integridad de la imagen para ambas particiones:

```
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
```

En la siguiente sección le guiaremos a través de los scripts que automatizan el proceso de verificación previa para todos los AP.

Script de comprobación previa

Sondeador WLAN(se puede descargar desde aquí)

Paso 1: Extraiga el sondeador WLAN a la ubicación de archivo deseada

Paso 2: Modifique estos valores en el archivo "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
```

Paso 3: Comente el resto del contenido predeterminado y la siguiente lista de comandos en los archivos "cmdlist_cos" y "cmdlist_cos_qca".

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

Muestra a continuación:

```
# 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
```

Paso 4: Ejecute el wlanpoller usando ".\wlanpoller.exe". El sondeador WLAN se ejecuta, envía SSH a todos los AP y obtiene las salidas de estos comandos para todos ellos.

Paso 5: Tras la ejecución, se crea una carpeta de "datos". Ingrese la carpeta y vaya hasta el final donde tiene varios archivos creados para cada AP.

Paso 6: Copie y pegue el archivo "ap_detection_script.py" proporcionado por separado en esta carpeta y ejecútelo. Puede encontrar el guion en el siguiente enlace de la caja:

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

Esto crea un archivo en la misma carpeta llamado "Status_check_results.log". Esto tiene la lista de AP que podrían estar potencialmente en un estado problemático y necesitarían algunos pasos adicionales de recuperación antes de continuar con su actualización.

Proceso de recuperación:

Basándose en el estado actual de cada punto de acceso que se determina que es problemático, el script proporcionaría más orientación sobre cuál sería la manera más optimizada de recuperar estos AP. Estos son los pasos detallados que debe seguir para cada una de las opciones.

Opción 1: Intercambio de particiones

Paso 1: Asegúrese de que el AP no tenga comunicación con el controlador para evitar que el AP vuelva a su partición/versión anterior. Esto se puede lograr a través de una lista de acceso en el gateway del controlador.

Paso 2: Desde los AP potencialmente afectados, configure el arranque para la partición 2:

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

Paso 3: Reinicie el AP para hacerlo arrancar con la imagen en la partición 2:

```
AP# reset
```

Paso 4: Haga que el AP se una al controlador después de que la actualización se complete en el controlador. El AP se une y descarga la nueva imagen.

NOTE: Si esta opción no es viable por cualquier razón, siempre puede abrir un caso TAC y continuar con la opción 2 para este conjunto de AP también.

Opción 2: Abra un caso del TAC para que el TAC limpie el AP del shell raíz (después de este proceso, continúe con la actualización normal)

Opción 3: Estado seguro, pero el AP tiene una imagen con errores en la partición de respaldo

Los AP terminan en este estado principalmente después de que se haya completado la actualización a una versión fija. Este estado sugiere que el AP está ejecutando una versión fija pero la versión de respaldo todavía está defectuosa. Para errar en el lado de la precaución, recomendamos reemplazar la copia de seguridad de los APs con una buena imagen también, es decir, una versión donde este problema no se ve. Dependiendo del número de AP en cuestión, archive descargue una imagen en el AP o simplemente haga una pre-descarga sin realmente activarla.

Opción 4: La comprobación de integridad de la imagen ha fallado para estos AP

Abra un caso del TAC para que el ingeniero del TAC rectifique estos AP antes de continuar con la actualización.

Opción 5: La comprobación de integridad de la imagen ha fallado para estos AP

La partición actual no es susceptible pero el almacenamiento flash es bajo. Se recomienda abrir un TAC para limpiar el cnssdaemon.log del almacenamiento a través del devshell.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).