Validar e recuperar APs Catalyst em 17.12 Afetados pela Falha de Atualização

Contents

Introdução

Este documento descreve o procedimento de recuperação quando você é afetado pelo bug da Cisco ID CSCwf25731 e CSCwf37271

Pontos de acesso afetados

Esses modelos de pontos de acesso são afetados. se não estiver usando os modelos abaixo, você não será afetado e não serão necessárias mais ações:

- 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)

Contexto

Os upgrades de sistemas que estiveram em 17.12.4/5/6a para qualquer versão podem fazer com que modelos específicos de pontos de acesso entrem em um loop de inicialização sob determinadas condições, acionados por falha de instalação da imagem devido a espaço em disco insuficiente no armazenamento do dispositivo de destino. Esse cenário ocorre somente durante uma operação de atualização envolvendo pontos de acesso, por exemplo, ISSU, instalação de imagem de controlador completo ou APSP, e não afeta nenhum serviço normal, operações diárias ou instalações SMU.

Etapas adicionais são necessárias antes de executar qualquer atualização nos pontos de acesso possivelmente afetados. Esse problema não tem solução alternativa e não depende de configuração, tipo de implantação ou modelo de controlador

Esse problema não afeta as versões anteriores à 17.12.4, ou se o Ponto de acesso estiver executando qualquer versão posterior à 17.12.6a, por exemplo, 17.15.x e nunca tiver instalado nenhuma das versões afetadas.

Uma correção está disponível para as versões 17.12.4, 17.12.5 e 17.12.6a do Cisco IOS XE, na forma dos respectivos APSPs. Além disso, um APSP de limpeza está disponível para 17.15.4d e 17.18.2, para recuperar o espaço perdido, para as implantações que estavam usando a versão impactada, e já atualizaram para uma versão posterior.

Se sua rede esteve em alguma das versões afetadas em algum momento ou se você não tiver certeza se a rede usou essas versões anteriormente, é recomendável executar as verificações antes de qualquer atualização como precaução

Detalhes da causa raiz

Os pontos de acesso dos modelos afetados, que executam os códigos 17.12.4 a 17.12.6a, criam um arquivo persistente "/storage/cnssdaemon.log", que pode crescer até 5 MB por dia, e usam todo o espaço disponível nessa partição de disco. Este arquivo não é limpo na reinicialização. Quando a partição estiver totalmente usada, os upgrades podem falhar, pois uma etapa crítica no armazenamento da nova versão do arquivo não é concluída.

O problema foi introduzido por uma atualização de biblioteca, que modificou o destino de log de um componente interno. O arquivo de log não é necessário para a operação do dispositivo

A falha de atualização só acontece se o AP estiver sendo executado da partição 1 e o espaço da partição 2 tiver sido esgotado. Se houver espaço suficiente ou se o AP tiver sido inicializado da partição 2, a atualização será bem-sucedida

Procedimento de verificação de atualização

Se a WLC estiver atualmente em17.12.4, 17.12.5, 17.12.6a, a atualização é obrigatória para uma versão de software com a correção enquanto segue as etapas abaixo. Para qualquer outra versão instalada na WLC, se estiver planejando atualizar,é altamente recomendável seguir estas instruções:

Passo 1: Verifique se os pontos de acesso são potencialmente afetados (consulte a Tabela 1). Se não for afetado, nenhum processo de pré-verificação/recuperação será necessário e você poderá prosseguir diretamente para atualizar para qualquer uma das versões mais recentes.

Passo 2: Se você for afetado, execute pré-verificações para identificar o número de APs afetados na seção Pré-verificações.

Passo 3: Nos AP identificados, execute as etapas de recuperação descritas na seção de recuperação.

Passo 4: Execute novamente a pré-verificação para confirmar que nenhum outro AP seja afetado.

Passo 5: Continue a atualizar para os respectivos APSPs ou versões de software mencionados na Tabela de versões fixas.

Consulte esta tabela para verificar se este aviso é aplicável a você:

Tabela 1 - Aplicabilidade do caminho de atualização

Versão atual	Destino	Aplicabilidade do Problema	Antes de atualizar, é necessário Pré-verificar	Caminho de Destino/Atualização	Pré-verificação de Atualização	Comentários
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	Verificar destino Notas de versão
17,9.x	Qualquer um (exceto 17.12.4/5/6a)	No	No	Siga o caminho de atualização de destino	No	17.9.1 a .5 não oferecem suporte à atualização direta para 17.15, use 17.9.6 ou

						superior Para obter mais informações, verifique as notas de versão
17.12.1 a 17.12.3	Qualquer (Exceto 17.12.4/5/6a)	No	No	Siga o caminho de atualização de destino	Processo regular	Verificar destino Notas de versão
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	Depois de instalar um APSP fixo, não são necessárias pré-verificações adicionais para atualizações futuras do 17.12
17.12.4/5/6a	17.15.x/17.18.x	Yes	Yes	Atualize o respectivo APSP 17.12.x e depois atualize para 17.15.x + APSPx ou 17.18.x + APSPx	Sim para a primeira atualização do APSP 17.12 e Não para as atualizações subsequentes.	
Qualquer versão, a imagem anterior era uma das 17.12.4/5/6a	17.15.x	Yes	Yes	17.15.x + APSPx	Yes	
Qualquer	17.18.x	Yes	Yes	17.18.x + APSPx	Yes	

versão, a imagem anterior era uma das 17.12.4/5/6a						
17,15+ Nova implantação	qualquer um	No	No	qualquer um	No	
17.18. Nova implantação	qualquer um	No	No	qualquer um	No	

Note: Em geral, se a rede não estiver em execução e não tiver executado 17.12.4, 17.12.5, 17.12.6a no passado, o problema não será aplicável

Note: Qualquer outra versão não mencionada explicitamente na coluna "Atual" segue o caminho de atualização recomendado.

Versões fixas

Controlador	Versão da imagem do 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

Pré-verificações

Para avaliar se a rede é susceptível a esse problema, execute as etapas atuais. Essas etapas ajudam a fornecer uma visão geral, mas para a detecção real de APs, use a seção "Scripts de pré-verificação" para automatizar esse processo:

- Confirme se as imagens do ponto de acesso são uma das versões afetadas, nas colunas de imagem Principal ou de Backup:

```
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
```

- Uma verificação semelhante pode ser realizada no 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
```

- Verifique a partição de inicialização atual:

```
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.
```

- Verifique o uso atual do sistema de arquivos:

```
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 a integridade da imagem para ambas as partições:

```
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
```

Na próxima seção, o guiaremos pelos scripts que automatizam o processo de pré-verificação para todos os APs.

Script de pré-verificação

Pesquisa de WLAN(Pode ser baixado aqui)

Passo 1: Extraia a pesquisa de WLAN para o local de arquivo desejado

Passo 2: Modifique estes valores no arquivo "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
```

Etapa 3: comente o restante do conteúdo padrão e a lista de comandos abaixo para os arquivos "cmdlist_cos" e "cmdlist_cos_qca".

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

Amostra abaixo:

```
# 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
```

Etapa 4: execute o wlanpoller usando ".\wlanpoller.exe". A pesquisa da WLAN é executada, SSH para todos os APs e obtém as saídas desses comandos para todos eles.

Passo 5: Após a execução, uma pasta de "dados" é criada. Insira a pasta e vá até o final, onde você tem vários arquivos criados para cada um dos APs.

Passo 6: Copie/cole o "ap_detection_script.py" fornecido separadamente nesta pasta e execute-o. Você pode encontrar o script no link da caixa abaixo:

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

Isso cria um arquivo na mesma pasta chamado "Status_check_results.log". Essa lista contém os APs que poderiam estar em um estado problemático e precisariam de algumas etapas de recuperação/extras antes de prosseguir com a atualização.

Processo de recuperação:

Com base no estado atual de cada ponto de acesso considerado problemático, o script forneceria orientação sobre qual seria a maneira mais otimizada de recuperar esses APs. Aqui estão as etapas detalhadas que você precisaria executar para cada uma das opções.

Opção 1: Troca de Partição

Passo 1: Certifique-se de que o AP não tenha comunicação com a controladora para evitar que o AP reverta para sua partição/versão anterior. Isso pode ser obtido por meio de uma lista de acesso no gateway do controlador.

Passo 2: A partir dos APs potencialmente afetados, configure a inicialização para a partição 2:

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

Passo 3: Reinicialize o AP para inicializá-lo com a imagem na partição 2:

```
AP# reset
```

Passo 4: Faça com que o AP se junte ao controlador após a atualização ser concluída no controlador. O AP entra e faz o download da nova imagem.

NOTE: Se essa opção não for viável por qualquer motivo, você sempre poderá abrir um caso de

TAC e continuar com a Opção 2 para esse conjunto de APs também.

Opção 2: Abra um caso de TAC para que o TAC limpe o AP do shell raiz (depois desse processo, você prossegue com a atualização normal)

Opção 3: Estado seguro, mas o AP tem uma imagem com bugs na partição de backup

Os APs terminam nesse estado principalmente após a atualização para uma versão fixa ter sido concluída. Esse estado sugere que o AP está executando uma versão fixa, mas a versão de backup ainda está com problemas. Para agir com cautela, recomendamos substituir o backup dos APs por uma boa imagem, ou seja, uma versão em que esse problema não seja visto. Dependendo do número de APs em questão, arquive o download de uma imagem para o AP ou apenas faça um pré-download sem ativá-lo.

Opção 4: A verificação de integridade da imagem falhou para esses APs

Abra um caso de TAC para que o engenheiro do TAC corrija esses APs antes de continuar com a atualização.

Opção 5: A verificação de integridade da imagem falhou para esses APs

A partição atual não é susceptível, mas o armazenamento em flash está baixo. É recomendável abrir um TAC para limpar o cnssdaemon.log do armazenamento através do devshell.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.