Atualizar Pontos De Acesso Com Segurança, Evitando Corrupção De Imagem Que Causa Loop De Inicialização

Contents

Introdução

Alguns access points (APs) da Cisco podem fazer download de uma imagem corrompida via CAPWAP de um controlador da série 9800. Dependendo da versão do software do AP, o AP pode tentar inicializar a imagem corrompida, resultando em um loop de inicialização. Este artigo explica quais modelos de AP e quais caminhos de rede são susceptíveis à corrupção de imagem e como atualizar com segurança.

Se seus APs agora estiverem em um loop de inicialização devido a esse problema, consulte o artigo Recuperar de um loop de inicialização causado pela corrupção de imagem nos access points Wave 2 e 11ax (CSCvx32806) para obter orientação sobre as etapas de recuperação.

Como Saber Se Uma Atualização É Susceptível A Corrupção De

Imagem

Seus APs podem ser susceptíveis a baixar software corrompido e, em seguida, tentar inicializar esse software, se as seguintes condições pertencerem à sua implantação:

Produtos não afetados

- Wireless LAN Controllers (WLCs): APs que fazem download a partir do AireOS Wireless LAN Controllers não são afetados
- Mobility Express, controlador sem fio integrado

- APs - Access Points Aironet 1800/1540/1100AC Series Wave 2 11ac e Wave1 11ac (1700/2700/3700/1570/IW3700) não são afetados (mesmo que esses APs estejam se registrando em 9800 Ws, eles não são afetados pelo LC)
- APs Wi-Fi 6E introduzidos desde 2023: IW9167, IW9165, C9163

Produtos afetados

- WLC : o download de APs dos Cisco Catalyst 9800 Series Wireless LAN Controllers pode ser afetado
- APs : Os seguintes modelos de AP registrados nos Cisco Catalyst 9800 Series Wireless LAN Controllers são afetados :
    - Access points Aironet Wave2 11ac (2800/3800/4800/1560/IW6330/ESW6300)
    - Pontos de acesso Catalyst 9100 Series Wi-Fi6 (9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
    - Pontos de acesso Catalyst 9100 Series Wi-FI6E (9136/9162/9164/9166)

Versões Afetadas: a Síndrome de Inicialização de Imagem Incorreta

Esse problema, em que o AP tenta inicializar uma imagem que sabe que está corrompida, é tratado pelos seguintes IDs de bug da Cisco: CSCvx32806, CSCwc72021, CSCwd90081, que são corrigidos nas seguintes versões:

- 8.10.185.0 e acima
- 17.3.7 e superior
- 17.6.6 e superior
- 17.9.3 e superior
- 17.11.1 e superior

Uma vez que o ponto de acesso é atualizado para o software com as correções acima, ele ainda pode baixar uma imagem corrompida; no entanto, ele não tentará inicializar essa imagem, mas continuará a tentar novamente o download até que seja bem-sucedido.

Caminhos de rede afetados

O problema de corrupção da imagem do AP não foi visto com um caminho de LAN entre o 9800 e

os APs - ou seja, caminhos com uma MTU IP completa de 1500 bytes, com baixa latência e perda de pacotes muito baixa não são afetados. É mais provável que o problema ocorra em túneis CAPWAP em uma WAN, com as seguintes características de caminho:

- alta perda de pacotes
- MTU de CAPWAP baixo (menos de 1485 bytes) - quanto menor o MTU, maior o risco
    - A baixa MTU do CAPWAP pode ser um sintoma de perda de pacotes

Como Saber Se O Caminho Da Rede Está Em Risco

- No 9800, verifique o MTU do caminho do CAPWAP com

```
<#root>

9800-L#show capwap detailed
Name          APMAC           SourceIP        SrcPort DestIP          DestPort

MTU

   Mode      McastIf
-------------------------------------------------------------------------------------------
Capwap1       D4AD.BDA2.8240 192.168.203.203 5247    192.168.6.100   5248

1485

  multicast Mc1
Capwap2       084F.F983.4A40 192.168.203.203 5247    192.168.6.103   5253

1005

  multicast Mc1
```

    - Se a MTU de um determinado AP estiver flutuando, isso será um forte indicador de risco
- Ou **show ap config general | incluir CAPWAP\ Caminho\ MTU** (em show tech-support wireless)
    - Use o Wireless Config Analyzer Express (WCAE) na saída "show tech-support wireless" do 9800 para ver a MTU dos APs em Access Points > Configuration
- No 9800, use "show ap uptime" e procure APs com um longo "AP Up Time" e um curto "Association Up Time"
    - Se não houver motivo para que os APs tenham um tempo de atividade de associação curto (ou seja, sem reconfiguração), isso pode indicar um caminho de rede em risco

Como atualizar com segurança a partir de uma versão de software de AP não fixo

---

Observação: se a sua implantação for susceptível à corrupção de imagem (isto é, modelos de AP afetados, execução de software sem a correção para a Síndrome de Inicialização de Imagem Ruim, com características de WAN de risco), não faça upgrade simplesmente atualizando o software 9800, e tendo os APs reingressando e baixando o novo software - eles podem estar sujeitos à corrupção de imagem e entrando em um loop de inicialização.

Em vez disso, use um destes métodos:

Atualizar usando uma WLC local para os APs

Se possível, coloque um controlador de preparação na LAN dos APs - isso poderia ser um 9800-CL ou (para APs Wave 2 / Wi-Fi 6) um AP no modo EWC e atualize os APs para a versão de destino. Eles poderão, então, entrar com segurança no controlador de produção.

Atualização via controlador AireOS

Se você tiver um controlador AireOS executando 8.10.190.0 ou superior, e se seus modelos de AP forem suportados pelo AireOS, junte os APs a esse controlador. Isso atualizará com segurança os APs para o software fixo e eles poderão, então, entrar com segurança no controlador de produção.

Atualizar usando archive download-sw

Prepare as imagens do AP de destino em um servidor TFTP/SFTP que seja acessível aos APs de atualização. As atualizações de imagem de AP via TFTP ou SFTP não estão sujeitas ao problema de corrupção de imagem. Os APs podem iniciar uma solicitação de download de imagem a partir da CLI do AP ou (se os APs estiverem unidos à controladora) a partir da CLI da controladora.

1. Configure um servidor TFTP ou SFTP em um local acessível aos APs. Observe que o desempenho do TFTP é restringido pela latência, portanto os downloads ficarão lentos se o servidor TFTP for remoto dos APs. Como o SFTP usa TCP, seu throughput será muito melhor se estiver usando um caminho de alta latência. No entanto, o SFTP não pode ser disparado da WLC, pois ele requer uma caixa de diálogo interativa para inserir o nome de usuário e a senha.
2. Prepare a(s) imagem(ns) do AP desejado(s) em um servidor TFTP ou SFTP. Consulte a Tabela 4 na Matriz de Compatibilidade da versão 15.3(3)J* do AP que mapeia para a versão IOS-XE desejada e, em seguida, faça o download das imagens apropriadas do Lightweight AP Software para os modelos de AP afetados em software.cisco.com.
    1. Por exemplo, a imagem 17.9.5 AP para um CW9162 isap1g6b-k9w8-tar.153-3.JPN4.tar.
3. Para atualizar via CLI do AP: se o CLI do AP estiver acessível via console ou SSH:
    1. Digite o comando TFTP ou SFTP:
       archive download-sw /no-reload tftp://<*ip-address*>/<*apimage*>
       or
       archive download-sw /no-reload sftp://<*ip-address*>/<*apimage*>
       Nome de usuário:*USER*
       Senha:*XXX*
       Isso substituirá a imagem corrompida pela imagem válida.
    2. Quando o download da imagem for concluído, emita:
       test capwap restart
       Isso reiniciará o processo CAPWAP, de modo que o AP reconheça a imagem recém-

instalada.

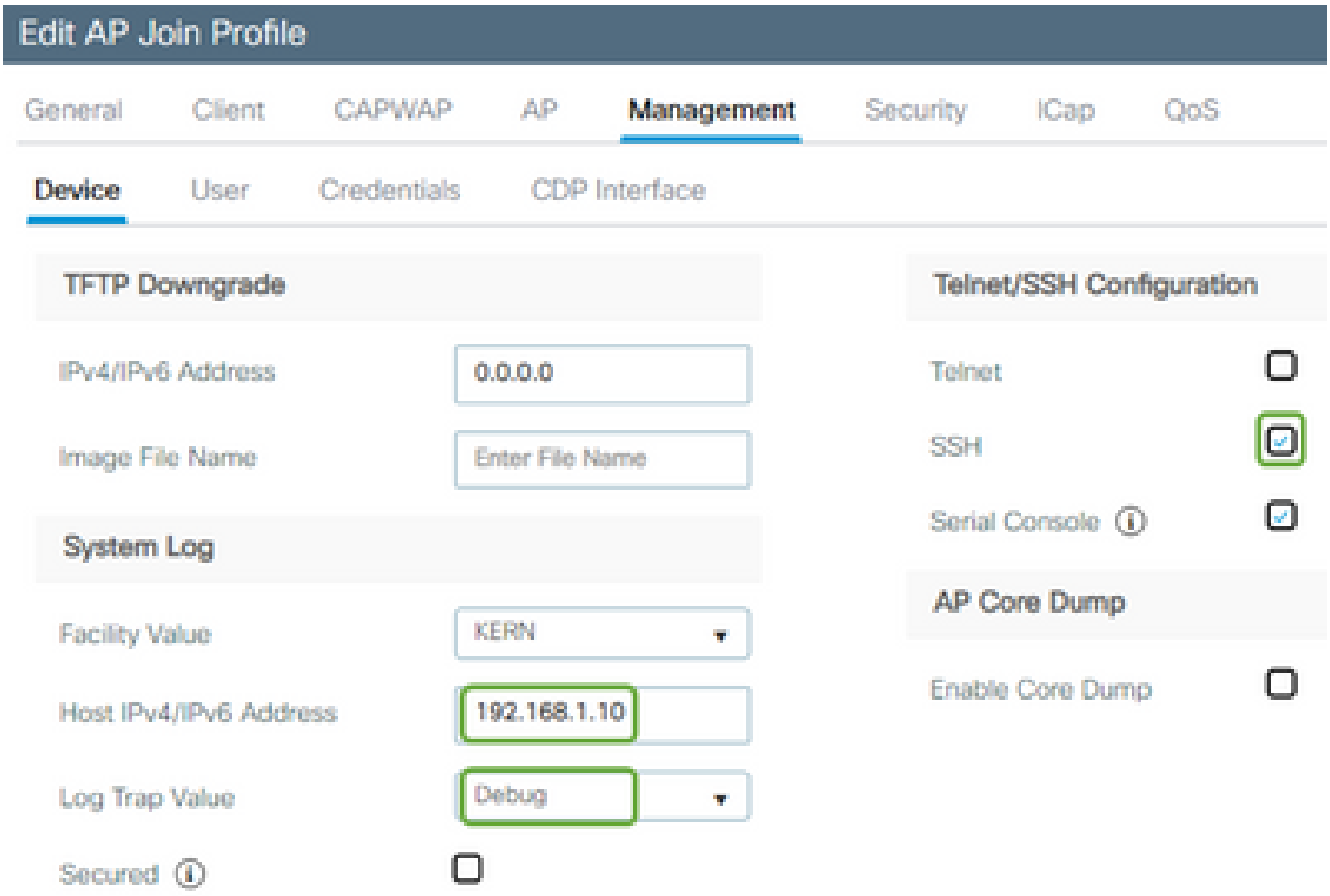
3. Para fazer upgrade de um grande número de APs via "archive download-sw", em vez de inserir o comando em cada AP individualmente, você pode usar um método de script. Consulte Upgrade APs Via WLAN Poller abaixo.

4. Se os APs estiverem unidos a uma controladora, você poderá atualizar os APs a partir da CLI da controladora (somente TFTP):
    1. No IOS-XE:**ap nameAPNAMEtftp-downgradeip.addr.of.server imagename.tar**
    2. No AireOS:**config ap tftp-*downgradeip.addr.of.server imagename.tarAPNAME***
        1. Embora os downloads do CAPWAP do AireOS não sejam susceptíveis a danos na imagem, se você estiver planejando migrar seus APs do AireOS para o 9800, você deve primeiro baixar uma imagem do AP com as correções para Alt-boot e a síndrome Boot a Bad Image (8.10.190.0 ou superior), antes de juntar os APs ao 9800.
    3. Monitore os logs do servidor TFTP ou SFTP para verificar se cada AP fez o download da imagem com êxito. Quando o download for concluído, cada AP será recarregado, executando a imagem recém-baixada.

Atualizar os APs via Pré-download, Monitoramento de erros

Carregue a imagem de destino no 9800 e use o pré-download do AP para enviar a nova imagem para o AP, enquanto monitora instâncias de corrupção de imagem do AP.

Etapa 1. Verifique se o SSH está habilitado sob o(s) perfil(is) de junção do AP na WLC C9800. Configure um Servidor syslog na rede. Configure o endereçoIP do Servidor syslog em AP Join Profile para todosos sites e defina o valor de armadilha de log como Debug. Verifique se o Servidor syslog está recebendo syslogs do AP.



Etapa 2. Faça o download da imagem do software para o C9800 WLC para se preparar para pré-download via CLI:

```
C9800# copy tftp://x.x.x.x/C9800-80-universalk9_wlc.17.03.07.SPA.bin bootflash:
C9800# install add file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
```

Etapa 3. Execute o pré-download da imagem do AP nas Cisco C9800 WLCs:

```
C9800# ap image predownload
```

Observação: dependendo da escala e do tipo de implantação, isso pode levar de alguns minutos a algumas horas. Não reinicialize o controlador ou os APs, até que você tenha validado que suas imagens são válidas!

Etapa 4. Uma vez que o pré-download de todos os APs tenha sido concluído, verifique se há uma destas duas mensagens de log no Servidor syslog:

- Êxito na verificação da assinatura da imagem.

- Falha na verificação da assinatura da imagem: -3

Além disso, verifique a saída do comando **`show ap image summary`**, verificando se há instâncias de Failed to Download. Se o contador for diferente de zero, localize os APs com falha por meio do comando show ap image | include Failed.

Cuidado: se algum AP registrar falha na verificação da assinatura da imagem, ou se algum AP falhar no download, NÃO CONTINUE COM O PROCESSO DE ATUALIZAÇÃO. Se todos os APs exibirem a mensagemImage signing verify success", todos os APs terão baixado corretamente a imagem e você poderá continuar com a atualização do 9800 com segurança.

Etapa 5. Se algum AP apresentou falha de verificação ou falhou no download, então, para evitar um loop de inicialização, você precisará sobrescrever a imagem na partição de Backup do AP com um download de arquivo de uma imagem separada do AP usando o seguinte processo.

Se o número de APs com falha for pequeno, você pode simplesmente executar SSH para cada AP e iniciar as seguintes etapas.

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

Observação: é necessário "reiniciar o comando test capwap" para que o processo CAPWAP do AP reconheça que a imagem na partição de backup foi atualizada. Isso causará uma breve interrupção do serviço, quando a conexão CAPWAP com o 9800 for reiniciada. Se essa for uma preocupação operacional, essa etapa pode ser adiada para uma janela de manutenção.

Atualizar APs usando a pesquisa de WLAN

Se o número de APs a serem atualizados via archive download-sw for grande, você poderá usar um processo automatizado usando a WLAN Poller.

Etapa 1a. Instale a pesquisa de WLAN em um Mac ou em uma máquina Windows.

Etapa 1b. Preencha o arquivo csv aplist com os APs com falha relevantes.

Etapa 1c. Preencha o arquivo cmdlist com os comandos abaixo (Você sempre pode adicionar mais conforme desejar):

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

Etapa 1d. Execute a pesquisa da WLAN.

Etapa 1e. Uma vez que sua execução tenha sido concluída, verifique cada arquivo de log do AP para validar a conclusão bem-sucedida.

Etapa 2. Ative imediatamente a imagem no C9800 WLC e recarregue.

```
C9800#install activate file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
- Confirm reload when prompted
```

Etapa 3. Comprometa a imagem no C9800 WLC. Ignorar esta etapa fará com que a WLC reverta para a imagem de software anterior

```
C9800#install commit
```

Perguntas mais freqüentes

P. Executei um pré-download há alguns dias, mas ainda não reinicializei meu Cisco C9800 WLC e APs. Não tenho syslogs para verificar se a imagem está corrompida. Como verifico se a imagem está corrompida?

R. Marque show logging nos APs/syslog. Se você não vir mensagens de êxito ou falha na saída do comando show logging, você pode usar o comando "show flash syslogs" para arquivar a saída do syslog de quando executou o pré-download. Se você vir a mensagem "Image signing verify success", então você sabe que este AP baixou a imagem com êxito.

P: Tenho uma implantação centralizada com APs no modo Local. Ainda preciso executar as etapas listadas na seção Solução alternativa/Soluções?

R: Esse problema foi relatado apenas durante a atualização de APs em uma conexão WAN. É muito improvável que os APs no modo Local e em redes locais tenham esse problema, portanto, não é necessário seguir esse procedimento para atualizações, se você tiver certeza de que há pouca perda de pacotes entre o controlador e os APs.

P: Tenho novos APs prontos para uso. Como posso implantá-los sem encontrar esse problema?

R: APs novos e prontos para fazer download de código pela WAN também estarão susceptíveis a esse problema, a menos que tenham sido fabricados após dezembro de 2023.

P: O que a Cisco está fazendo a longo prazo para resolver esse problema com downloads de imagens CAPWAP do 9800 sendo corrompidos?

R: Uma vez que o AP já esteja executando o 17.11 ou superior, ele pode usar o recurso Out-of-

Band Image Download (Download de imagem fora da banda) para extrair a imagem do controlador usando HTTPS. O TCP transmite dados de forma confiável, usando uma janela deslizante - portanto, também é muito mais rápido em uma WAN do que o CAPWAP (ou TFTP)

P. Tenho APs que agora estão em um loop de inicialização. Como posso recuperá-los?

R: Consulte o artigo Recuperação de um loop de inicialização causado por corrupção de imagem em access points Wave 2 e 11ax (CSCvx32806
).

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.