Falha no download da imagem do IOS AP devido ao certificado de assinatura de imagem expirado após 4 de dezembro de 2022 (CSCwd80290)

Contents

Introduction

Este documento fornece detalhes sobre falhas de junção do ponto de acesso (AP) do IOS, observadas com as controladoras Wireless LAN (WLCs) AireOS e C9800, após 4 de dezembro de 2022. Esse problema é rastreado pelo bug Cisco CSCwd80290 e pelo Field Notice FN72524 e é causado por uma falha de validação de certificado de assinatura de imagem AP.

Produtos afetados

Esse problema afeta todos os pontos de acesso lightweight que executam o IOS - eles incluem: APs 802.11ac Wave 1 (séries IW3702/3700/2700/1700/1570) e APs anteriores, incluindo 700/1530/1550/3600/2600/1600/3500/AP8 Série 02/AP803. As imagens IOS leves afetadas foram criadas de dezembro de 2012 a novembro de 2022. AireOS, Catalyst 9800 Series e controladores de acesso convergente são afetados. Os APs que executam AP-COS (APs 802.11ac Wave 2, Wi-Fi 6, Wi-Fi 6E) não são afetados, nem os APs IOS estão em modo autônomo.

Problema

Quando os APs do IOS são atualizados ou desatualizados via CAPWAP, após 4 de dezembro de 2022, eles podem ficar presos em um loop de download de imagem e, portanto, não se unir à

WLC, devido a uma falha na validação do certificado de assinatura na imagem descarregada.

Causa raiz

Os certificados de assinatura de imagem agrupados nas imagens do AP IOS foram emitidos em 4 de dezembro de 2012 e expiraram em 4 de dezembro de 2022. Os APs IOS usam esse certificado para validar a imagem baixada da WLC, antes de instalar o software no AP. Assim, após 4 de dezembro de 2022, quando um AP faz o download do código devido a atualização/downgrade de software ou devido à mudança entre WLCs que executam versões diferentes, o AP falhará em validar a imagem e permanecerá em um loop de imagem de download indefinidamente. O problema é observado em todas as versões do AireOS e do IOS-XE.

Sintomas

Para verificar se você está enfrentando esse problema, primeiro verifique na WLC se há APs presos no status de download. Em seguida, para identificar positivamente o problema, ssh, telnet ou console nos APs afetados e exibir seus logs (ou procurar logs de AP no seu Servidor syslog).

Em uma WLC AireOS

Na WLC, **show ap image status** (AireOS 8.10) mostrará os APs afetados no status "Downloading".

Na versão 8.5, use **show ap image all**, que mostrará um número diferente de zero de APs em "Downloading".

```
(AireOS WLC-8.5) >show ap image all Total number of APs..... 1 Number
of APs Initiated..... 0
Downloading..... 1
Predownloading..... 0 Completed
predownloading..... 0 Not Supported..... 0
Failed to Predownload..... 0 Predownload Predownload Flexconnect AP Name
Primary Image Backup Image Status Version Next Retry Time Retry Count Predownload --------------
---- -------------- -------------- --------------- -------------- ---------------- ------------
-------------- AP1700 8.5.182.0 0.0.0.0 None None NA NA (AireOS WLC-8.10) >show ap image status
Total number of APs..... X Total AP's
Downloading..... 1 AP Name Primary Image Download Status -----------------
- -------------- ---------------- CAP3702E.4CD4 17.3.6.76 Downloading
```

Em uma WLC IOS-XE C9800

C9800#show ap summary

```
9800-L#show ap summary AP Name Slots AP Model Ethernet MAC Radio MAC Location Country IP Address
State ------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
- AP2702E 2 2702E 0081.c4fb.2e74 843d.c673.10d0 default location 192.168.202.105 Downloading
```

Os registros AP mostrarão erros semelhantes aos seguintes ao encontrar esse problema:

Em um AP SHA-1 (fabricado antes de meados de 2014):

```
*Dec 6 21:35:24.259: Using SHA-1 signed certificate for image signing validation.
*Dec 6 21:35:24.327: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has
failed. The certificate (SN: XX) has expired. Validity period ended on 21:37:36 UTC Dec 4 2022
*Dec 6 21:35:24.327: Image signing certificate validation failed (1A).
*Dec 6 21:35:24.327: Failed to validate signature
*Dec 6 21:35:24.327: Digital Signature Failed Validation (flash:/update/ap3g2-k9w8-mx.153-
3.JPJ9/final_hash)
*Dec 6 21:35:24.327: AP image integrity check FAILED
```

Em um AP SHA-2 (fabricado após meados de 2014):

```
*Dec 6 08:47:20.159: Using SHA-2 signed certificate for image signing validation.
*Dec 6 08:47:20.223: DTLS_CLIENT_ERROR: ../capwap/base_capwap/dtls/base_capwap_dtls_record.c:169
Pkt too old last_seq_num : 11116,Received sequence num: 1 distance: -11115
*Dec 6 08:47:20.227: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has
failed. The certificate (SN: XX) has expired. Validity period ended on 21:43:46 UTC Dec 4 2022
*Dec 6 08:47:20.227: Image signing certificate validation failed (1A).
*Dec 6 08:47:20.231: Failed to validate signature
*Dec 6 08:47:20.231: Digital Signature Failed Validation (flash:/update/ap3g2-k9w8-mx.153-
3.JPJ7c/final_hash)
*Dec 6 08:47:20.231: AP image integrity check FAILED
```

Solução

Se você não estiver executando um software fixo, siga estas etapas para permitir que os APs IOS se unam.

1. Desative o NTP para impedir que o controlador defina automaticamente seu tempo de encaminhamento.

```
AireOS: (AireOS WLC)>show time make a note of all configured NTP servers, and delete each one:
(AireOS WLC)>config time ntp delete
```

2. Altere a data na WLC para algo antes de 4 de dezembro de 2022, mas não antes de 1 de novembro de 2022, pois ela pode invalidar o certificado na controladora ou em APs mais recentes.

```
(AireOS WLC)> config time manual 12/02/22 00:00:00 C9800#clock set 00:00:00 2 Dec 2022
```

3. Verifique se a hora na WLC mudou

```
(AireOS WLC)> show time Time..................................... Fri Dec 2 00:00:02
2022 C9800#show clock 00:00:02.573
```

4. Aguarde até que todos os APs apareçam no estado Registered com a nova imagem.

> **Observação: em alguns casos, uma reinicialização do AP pode ser necessária após a alteração da data para que o AP seja unido. Mas certifique-se de esperar pelo menos 30 minutos para permitir que o AP se junte novamente antes de reinicializar os APs**

5. Ative o NTP novamente

```
(AireOS WLC)>config time ntp server 1
```

6. Salve a configuração

```
(AireOS WLC)>save config Are you sure you want to save? (y/n) y C9800#write memory
```

7. Verifique novamente o relógio na WLC

```
(AireOS WLC)>show time C9800# show clock
```

Atualizando para software fixo

Em uma WLC AireOS

1. Se você tiver qualquer AP preso no download, defina o tempo do controlador novamente para que os APs possam concluir o download e entrar no estado Registered antes de atualizar para o software. Consulte a seção de solução alternativa acima para obter detalhes sobre como definir o tempo de retornoSe, por razões operacionais, você não puder definir o tempo de volta, bloqueie os APs IOS afetados de tentar se unir ao controlador, por exemplo, desligando suas portas de switch ou instalando uma ACL para bloquear o CAPWAP.
2. Agora que nenhum AP está no estado Downloading (Baixando), certifique-se de que a hora da WLC esteja definida para a hora atual (reative o NTP).
3. Instale o software fixo no AireOS WLC (8.10.183.0 ou superior; ou, se não for possível atualizar do 8.5, use 8.5.182.7, se estiver usando 8.5 mainline, ou 8.5.182.105, para 8.5 IRCM.). Consulte os links abaixo para baixar o software fixo. 8.10 8540: https://software.cisco.com/download/home/286284728/type/280926587/release/8.10.183.0 5520: https://software.cisco.com/download/home/286284738/type/280926587/release/8.10.183.0 3504: https://software.cisco.com/download/home/286312601/type/280926587/release/8.10.183.0 vWLC: https://software.cisco.com/download/home/284464214/type/280926587/release/8.10.183.08. 5 (postagens ocultas) 8.5.182.7 (linha principal 8.5): https://software.cisco.com/download/specialrelease/8f166c6d88b9f77aabb63f78affa9749. 8.5.182.105 (8.5 IRCM): https://software.cisco.com/download/specialrelease/bc334964055fbd9440834f008e5aca34.
4. (Opcionalmente) Antes de reinicializar, faça o download prévio do software fixo para os APs associados.
5. Reinicializar a WLC.
6. Se você desativou as portas de switch do AP ou bloqueou o CAPWAP, remova os blocos para permitir que os APs do IOS ingressem novamente e façam o upgrade.

Em uma WLC IOS-XE 9800

1. Faça o download do software IOS-XE 17.3.6, 17.6.4 e 17.9.2 para a memória flash 9800. Consulte as versões recomendadas do IOS-XE para WLCs C9800 para escolher a versão mais adequada para seu ambiente com base nos modelos AP em seu ambiente e nos recursos em uso.

2. Descarregue o arquivo 17.3.6 APSP7 ou 17.6.4 APSP1 ou 17.9.2 APSP1 (com correção IOS

AP) para a flash 9800.

- 17.3.6: 17.3.6 APSP7 via CSCwd83653/CSCwe10047 (correção também incluída em APSP2 e APSP5)

9800-40: https://software.cisco.com/download/home/286316412/type/286325254/release/17.3.6

9800-80: https://software.cisco.com/download/home/286321396/type/286325254/release/17.3.6

9800-CL: https://software.cisco.com/download/home/286322605/type/286325254/release/17.3.6

9800-L: https://software.cisco.com/download/home/286323430/type/286325254/release/17.3.6

- 17.6.4: 17.6.4 APSP1 (para IW3702) via CSCwd87305

9800-40: https://software.cisco.com/download/home/286316412/type/286325254/release/17.6.4

9800-80: https://software.cisco.com/download/home/286321396/type/286325254/release/17.6.4

9800-CL: https://software.cisco.com/download/home/286322605/type/286325254/release/17.6.4

9800-L: https://software.cisco.com/download/home/286323430/type/286325254/release/17.6.4

- 17.9.2:17.9.2 APSP1 (para IW3702) via CSCwd87612

9800-40: https://software.cisco.com/download/home/286322605/type/286325254/release/17.9.2

9800-80: https://software.cisco.com/download/home/286321396/type/286325254/release/17.9.2

9800-CL: https://software.cisco.com/download/home/286322605/type/286325254/release/17.9.2

9800-L: https://software.cisco.com/download/home/286323430/type/286325254/release/17.9.2

Note:
1) 17.3.6 APSP7 inclui correções para vários bugs (CSCvx32806, CSCwc32182, CSCvz99036, CSCwd37092, CSCwc78435, CSCwc88148) além do CSC wd80290
2) 17.6.4 APSP1 inclui correções para vários bugs (CSCwc73090, CSCwc71198, CSCwc78435, CSCwd40731, CSCvx32806) além de CSCwd80290 (para IW 3700).

3. A menos que o 17.3.6 já esteja instalado, instale o 17.3.6 IOS-XE agora e recarregue.

```
C9800#install add file bootflash:/C9800-L-universalk9_wlc.17.03.06.SPA.bin activate commit
```

4. Após a reinicialização do 9800 - se a hora da controladora tiver sido redefinida no tempo, defina agora sua hora como atual (reative o NTP.)

5 Instale o APSP7 para recuperar os APs IOS:

```
C9800#install add file bootflash:/C9800-universalk9_wlc.17.03.06.CSCwe10047 .SPA.apsp.bin
C9800#install activate file bootflash:/C9800-universalk9_wlc.17.03.06.CSCwe10047 .SPA.apsp.bin
C9800#install commit
```

Perguntas frequentes

- **Meus APs registrados atuais vão se desconectar ou não ingressar devido a esse problema?**
  Os APs que executam a mesma versão que a WLC continuarão a operar sem problemas e inicializarão e se juntarão normalmente. Esse problema afeta apenas o processo de validação de imagem feito como parte de uma atualização de imagem.

- **O pré-download do AP é afetado?**

Yes. Como o pré-download do AP envolve o download de uma imagem para o AP e a validação da imagem pelo AP, o mesmo certificado expirado e a falha de validação da imagem são encontrados.

- **Qual é o impacto no serviço causado pela mudança de horário? Um cliente pode fazer isso ao meio-dia ou deve programar uma janela de manutenção com algum tempo de inatividade e impacto nos serviços?**
  Alterar a hora do controlador não tem impacto operacional nas junções de APs e na conectividade do cliente sem fio. No entanto, os espaços do DNA Center Assurance, CMX e Cisco (DNA) podem ser afetados. Depois que os APs são unidos e a hora é ajustada para a hora atual, espera-se que esses serviços sejam recuperados.

- **E se eu não puder definir a hora de volta no meu controlador de produção?**
  Configure uma WLC de preparação (vWLC ou 9800-CL também funciona) com a mesma versão de código da WLC de produção. Reverta o tempo na WLC de preparo e junte os APs à WLC de preparo. Quando os APs baixarem o código e passarem para o estado Registered na WLC de preparação, mova os APs para a WLC de produção.

- **Preciso alterar o horário para instalar a versão fixa?**

Somente com o AireOS, se os APs estiverem presos no estado de download. Consulte a seção sobre *Upgrade para software fixo* para obter mais detalhes.

- **O que acontece se eu adicionar um novo AP?**
  Se o novo AP tiver instalado nele a mesma versão que a controladora, o AP deverá se unir sem problemas.
  Por outro lado, se a versão não coincidir, o AP tentará baixar a imagem correspondente. Se o código no controlador não tiver as imagens do pacote de AP fixo, isso fará com que o AP falhe na atualização, conforme descrito, e a solução alternativa será necessária.
  Se o controlador tiver sido atualizado para uma das versões fixas, novos APs poderão ser adicionados normalmente e conclua o processo de atualização.

- **O que acontecerá com as unidades recebidas da RMA?**
  Isso equivale a adicionar um novo AP: se você estiver executando a versão do controlador com a correção da imagem do AP, eles se juntarão e atualizarão normalmente.
  Caso contrário, aplique a solução de tempo.

- **Preciso manter a hora modificada para a operação?**
  Não, uma vez que os APs tenham concluído o processo de atualização, você pode redefinir o controlador para a hora atual e reativar o NTP.

- **Estou vendo este erro no log de AP %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID:**

Falha na validação da cadeia de certificados. O certificado (SN: xx) ainda não é válido O período de validade começa em HH:MM:SS UTC 1 de março de 2022". Este é o mesmo sintoma ou um novo sintoma?

Esse erro indica que o relógio na WLC está definido para depois de 1º de março de 2022, que é a data de início do certificado (nesse caso). Essa data varia dependendo de quando a WLC foi fabricada ou quando o certificado autoassinado na WLC virtual foi gerado.

Modifique o relógio na WLC para tornar o certificado válido.

- **O que a Cisco está fazendo para evitar que esse problema se repita?**
  Estamos concluindo uma auditoria completa em todos os produtos corporativos, para identificar qualquer problema semelhante que possa não ter sido detectado e implementar ações corretivas
  Além disso, foram aplicadas alterações ao processo de pacote de imagem do IOS AP para corrigir esse problema.

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.