Solucionar problemas de segurança, certificado e vulnerabilidade do ASDM TLS

Contents

Introdução

Este documento descreve o processo de solução de problemas de segurança, certificado e vulnerabilidade do ASDM Transport Layer Security (TLS).

Background

O documento faz parte da série de solução de problemas do Adaptive Security Appliance Device Manager (ASDM) juntamente com estes documentos:

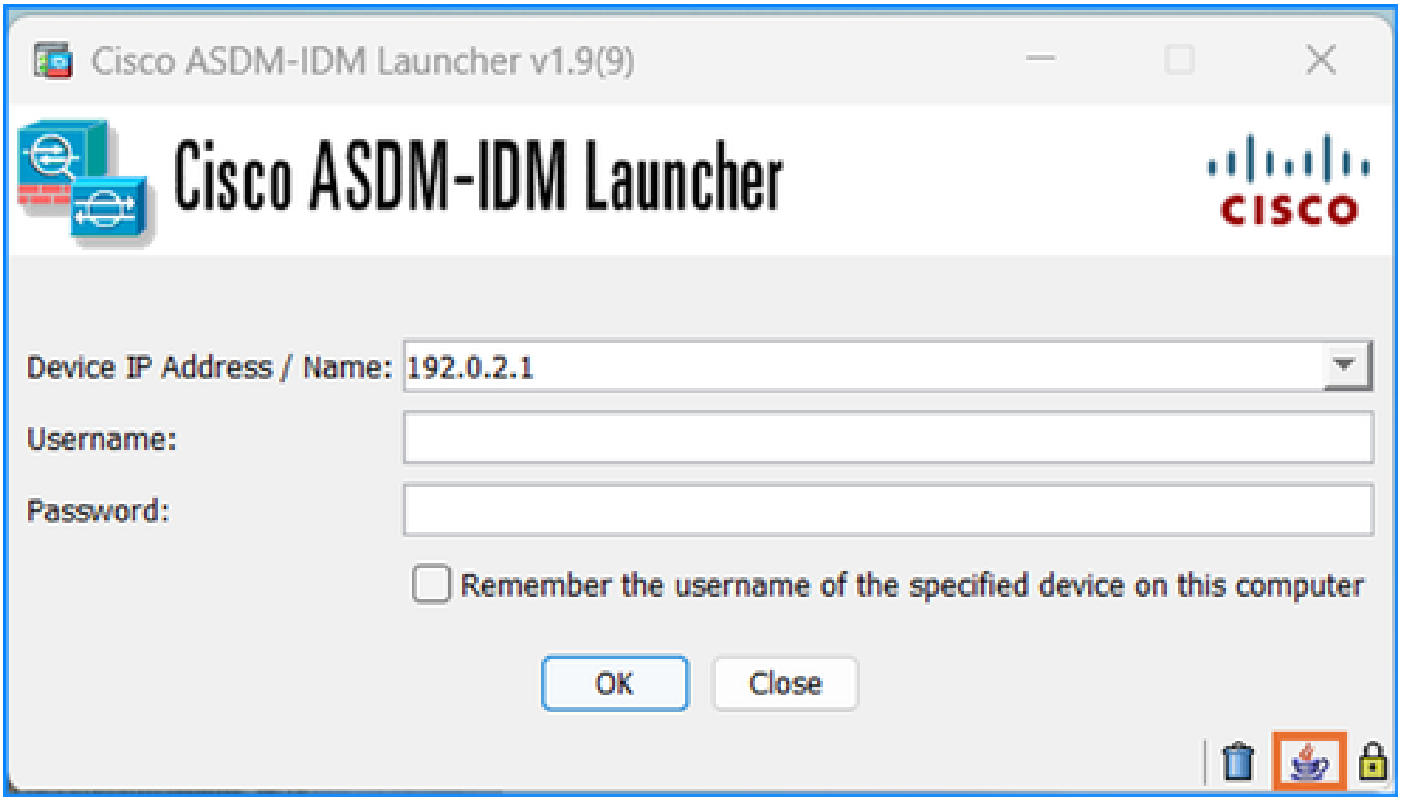
- Identificar e Solucionar Problemas de Inicialização do ASDM
- Solucionar Problemas de Configuração, Autenticação e Outros Problemas do ASDM
- Solucionar Problemas de Licença, Atualização e Compatibilidade do ASDM

Problemas de criptografia TLS ASDM

Problema 1. O ASDM não pode se conectar ao firewall devido a problemas de cifra TLS

O ASDM não pode se conectar ao firewall. Um ou mais destes sintomas são observados:

- O ASDM mostra as mensagens de erro "Não foi possível abrir o dispositivo" ou "Não foi possível iniciar o gerenciador de dispositivos do <ip>".
- A saída do comando show ssl error contém o erro de biblioteca SSL. Função: ssl3_get_client_hello Motivo: no shared cipher" message.
- Os registros do console Java mostram a "javax.net.ssl.SSLHandshakeException: Alerta fatal recebido: mensagem de erro handshake_failure":



<#root>

```
javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure


   at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
   at sun.security.ssl.Alerts.getSSLException(Alerts.java:154)
   at sun.security.ssl.SSLSocketImpl.recvAlert(SSLSocketImpl.java:2033)
```

Solução de problemas - Ações recomendadas

Uma causa raiz comum dos sintomas é a falha de negociação do conjunto de cifras TLS entre o ASDM e o ASA. Nesses casos, dependendo da configuração de codificação, o usuário precisa ajustar o certificado no lado ASMD e/ou ASA.

Siga uma ou mais destas etapas até que a conectividade seja bem-sucedida:

1. No caso do ASDM com OpenJRE, se conjuntos de cifras TLS fortes forem usados, aplique a solução do bug do software Cisco ID CSCv12542 "O ASDM open JRE deve usar cifras mais altas por padrão":
2. Iniciar Bloco de Notas (executar como administrador)
3. Abra o arquivo: C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security
4. Procurar: crypto.policy=ilimitado
5. Remova # na frente dessa linha para que todas as opções de criptografia fiquem disponíveis
6. Save

2. Altere os conjuntos de cifras TLS no ASA.

<#root>

```
ASA(config)#
```

ssl cipher ?

```
configure mode commands/options:
  default   Specify the set of ciphers for outbound connections
  dtlsv1    Specify the ciphers for DTLSv1 inbound connections
  dtlsv1.2  Specify the ciphers for DTLSv1.2 inbound connections
  tlsv1     Specify the ciphers for TLSv1 inbound connections
  tlsv1.1   Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2   Specify the ciphers for TLSv1.2 inbound connections
  tlsv1.3   Specify the ciphers for TLSv1.3 inbound connections
```

As opções de codificação para TLSv1.2:

<#root>

```
ASA(config)#
```

ssl cipher tlsv1.2 ?

```
configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration string.
```

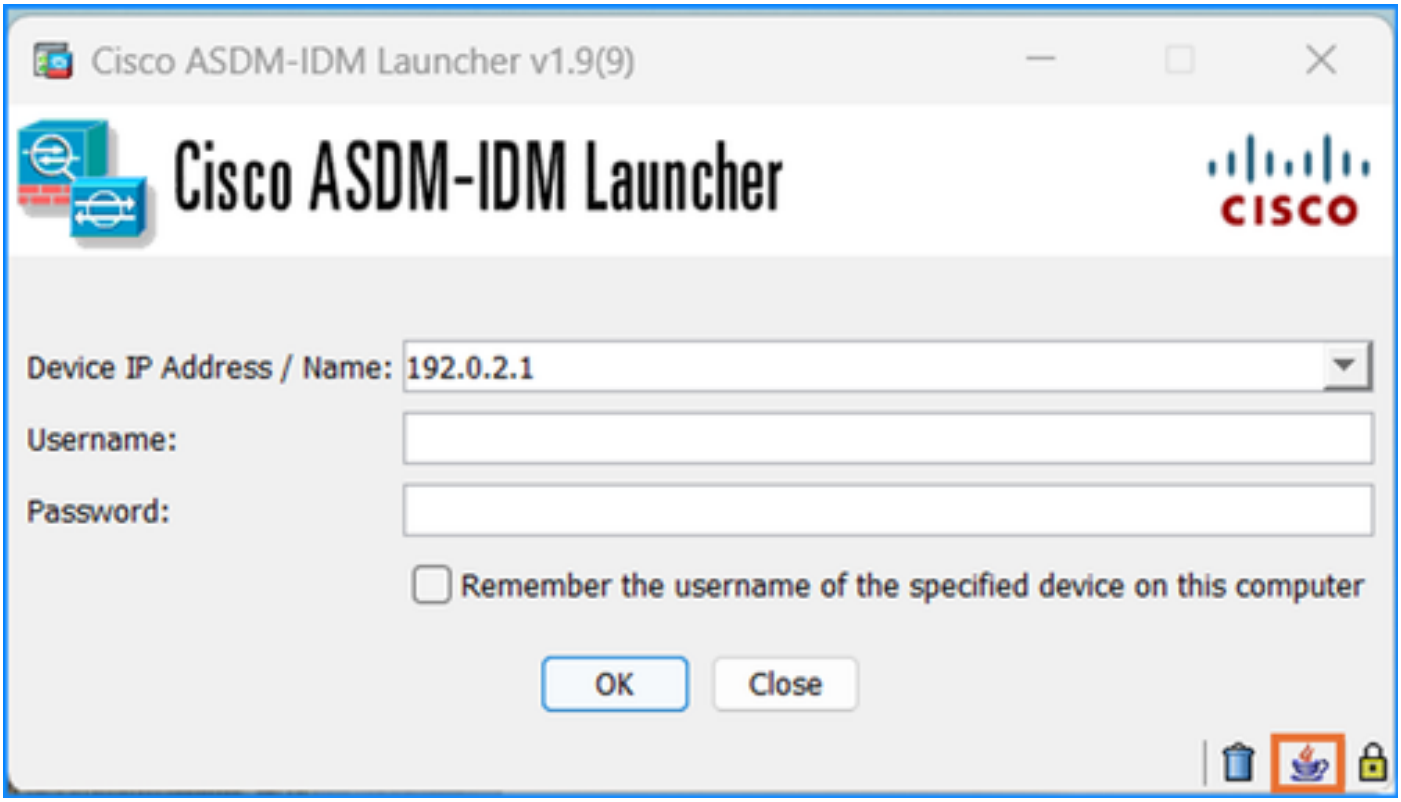
---

aviso: As alterações no comando ssl cipher são aplicadas ao firewall inteiro, incluindo as conexões VPN de site para site ou de acesso remoto.

Problema 2. O ASDM não pode se conectar ao devido à falha de handshake TLS1.3

O ASDM não pode se conectar ao devido à falha de handshake TLS1.3.

Os registros do console Java mostram a "java.lang.IllegalArgumentException: Mensagem de erro TLSv1.3":



<#root>

```
java.lang.IllegalArgumentException: TLSv1.3

at sun.security.ssl.ProtocolVersion.valueOf(Unknown Source)
              at sun.security.ssl.ProtocolList.convert(Unknown Source)
              at sun.security.ssl.ProtocolList.<init>(Unknown Source)
              at sun.security.ssl.SSLSocketImpl.setEnabledProtocols(Unknown Source)
              at sun.net.www.protocol.https.HttpsClient.afterConnect(Unknown Source)
```

Solução de problemas - Ações recomendadas

A versão TLS 1.3 deve ser suportada no ASA e no ASDM. O TLS versão 1.3 é suportado nas versões 9.19.1 e posteriores do ASA (Release Notes for the Cisco Secure Firewall ASA Series, 9.19(x)). O Oracle Java versão 8u261 ou posterior é necessário para suportar TLS versão 1.3 (Release Notes for Cisco Secure Firewall ASDM, 7.19(x)).

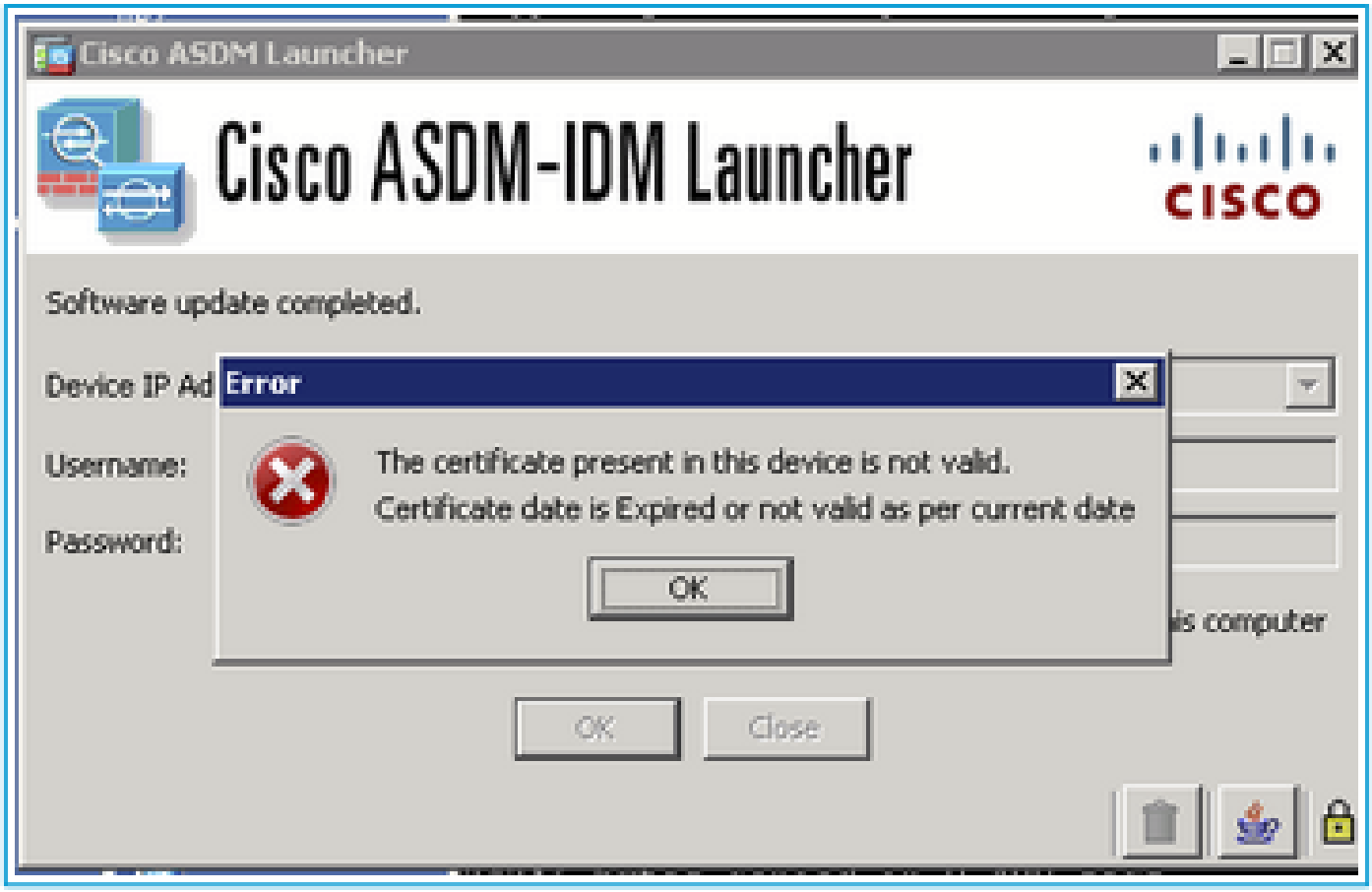
Referências

1. Notas de versão do Cisco Secure Firewall ASA Series, 9.19(x)
2. Notas de versão do Cisco Secure Firewall ASDM, 7.19(x)

Problemas de Certificado ASDM

Problema 1. "O certificado presente neste dispositivo não é válido. A data do certificado expirou ou não é válida de acordo com as datas atuais." mensagem de erro

A mensagem de erro é mostrada ao executar o ASDM: "O certificado presente neste dispositivo não é válido. A data do certificado expirou ou não é válida de acordo com as datas atuais."



Sintomas semelhantes são descritos nas notas de versão:

"O certificado autoassinado do ASDM não é válido devido a uma incompatibilidade de data e hora com o ASA — o ASDM valida o certificado SSL autoassinado e, se a data do ASA não estiver dentro da data Emitido em e Expira em do certificado, o ASDM não será iniciado. Consultar Notas de compatibilidade do ASDM

Solução de problemas - Ações recomendadas

1. Verificar e confirmar certificados expirados:

<#root>

#

show clock

10:43:36.931 UTC Wed Nov 13 2024

<#root>

#

show crypto ca certificates

```
Certificate
  Status: Available
  Certificate Serial Number: 673464d1
  Certificate Usage: General Purpose
  Public Key Type: RSA (4096 bits)
  Signature Algorithm: RSA-SHA256
  Issuer Name:
    unstructuredName=asa.lab.local
    CN=CN1
  Subject Name:
    unstructuredName=asa.lab.local
    CN=asa.lab.local
  Validity Date:
    start date: 10:39:58 UTC Nov 13 2011
    end   date: 10:39:58 UTC Nov 11 2022
  Storage: config
  Associated Trustpoints: SELF-SIGNED
  Public Key Hashes:
   SHA1 PublicKey hash:   b9d97fe57878a488fad9de99186445f45187510a
   SHA1 PublicKeyInfo hash: 29055b2efddcf92544d0955f578338a3d7831c63
```

1. Na CLI (Command Line Interface, interface de linha de comando) do ASA, remova a linha ssl trust-point <cert> <interface>, onde <interface> é o nome usado para conexões ASDM. O ASA usa o certificado autoassinado para conexões ASDM.
2. Se não houver um certificado autoassinado, gere um. Neste exemplo, o nome SELF-SIGNED é usado como um nome de ponto verdadeiro:

<#root>

conf t

crypto ca trustpoint SELF-SIGNED

enrollment self

fqdn

subject-name CN=

,O=

,C=

,St=

,L=

```
exit

crypto ca enroll SELF-SIGNED

crypto ca enroll SELF-SIGNED

WARNING: The certificate enrollment is configured with an




that differs from the system fqdn. If this certificate will be

used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be: asa.lab.local

% Include the device serial number in the subject name? [yes/no]:

Generate Self-Signed Certificate? [yes/no]: yes
```

3. Associe o certificado gerado à interface:

<#root>

ssl trust-point SELF-SIGNED

4. Verifique o certificado:

<#root>

#

show crypto ca certificates

```
Certificate
  Status: Available
  Certificate Serial Number: 673464d1
  Certificate Usage: General Purpose
  Public Key Type: RSA (4096 bits)
  Signature Algorithm: RSA-SHA256
  Issuer Name:
    unstructuredName=asa.lab.local
    CN=CN1
  Subject Name:
    unstructuredName=asa.lab.local
    CN=CN1
  Validity Date:
    start date: 12:39:58 UTC Nov 13 2024
    end   date: 12:39:58 UTC Nov 11 2034
  Storage: config
  Associated Trustpoints: SELF-SIGNED
  Public Key Hashes:
   SHA1 PublicKey hash:     b9d97fe57878a488fad9de9912sacb3772777
   SHA1 PublicKeyInfo hash: 2955b2efdd3737c8bb335f578338a3d7831c63
```

5. Verifique a associação do certificado com a interface:

<#root>

```
#
 show run all ssl
```

Problema 2. Como instalar ou renovar certificados usando o ASDM ou o ASA CLI?

Os usuários querem esclarecer as etapas para instalar ou renovar certificados usando o ASDM ou a CLI do ASA.

Ações recomendadas

Consulte os guias para instalar e renovar certificados:

- ASA: Instalação e renovação do certificado digital SSL
- Instalar e renovar certificados no ASA gerenciado pela CLI

Problemas de vulnerabilidade do ASDM

Esta seção aborda os problemas mais comuns relacionados à Vulnerabilidade do ASDM.

Problema 1. Vulnerabilidade detectada no ASDM

Caso detecte uma vulnerabilidade no ASDM.

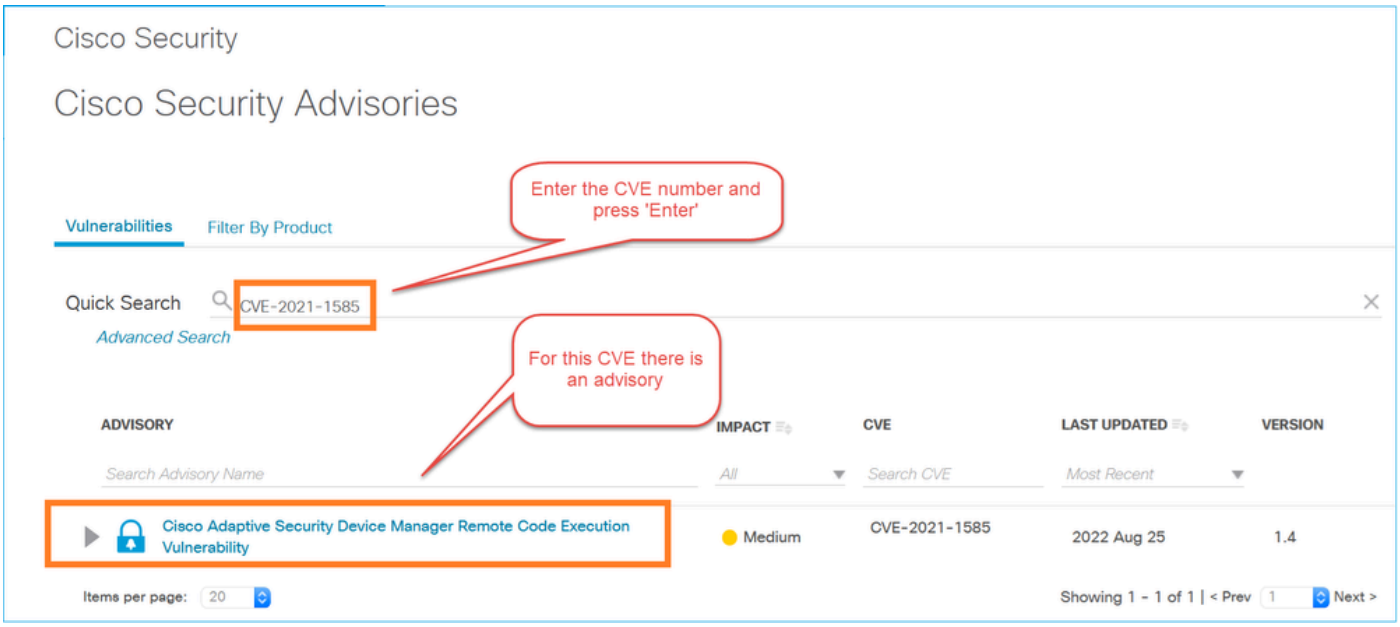
Solução de problemas - Etapas recomendadas

Passo 1: Identifique a ID do CVE (por exemplo, CVE-2023-21930)

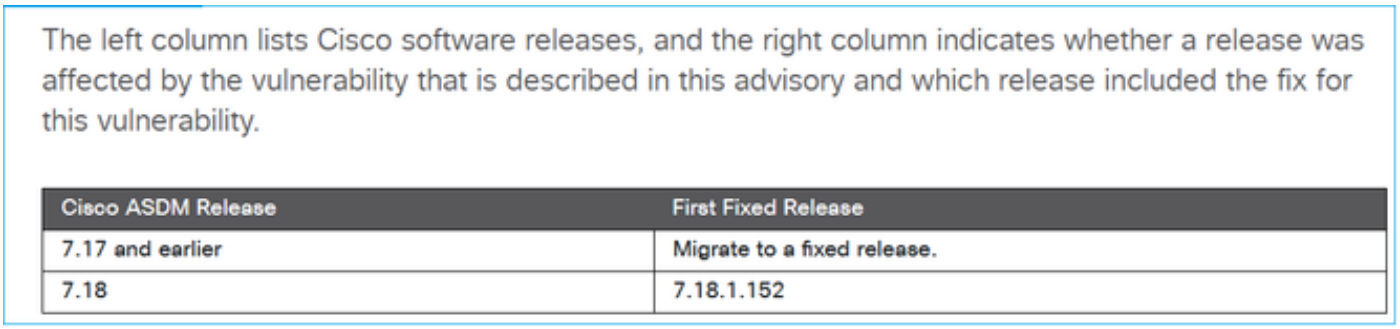
Passo 2: Procure o CVE nas Cisco Security Advisories e na ferramenta Cisco Bug Search:

Navegue até a página de recomendação:

https://sec.cloudapps.cisco.com/security/center/publicationListing.x



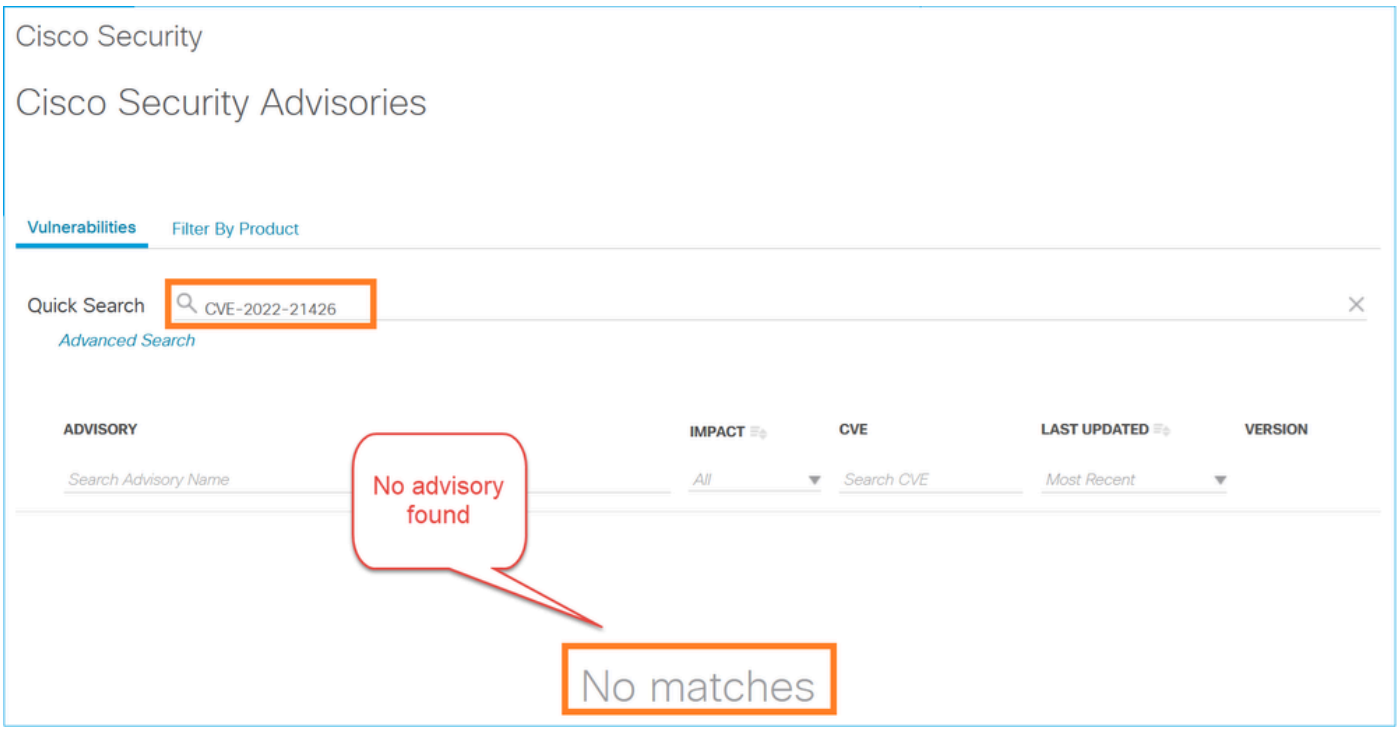
Abra a recomendação e verifique se o ASDM é afetado, por exemplo:

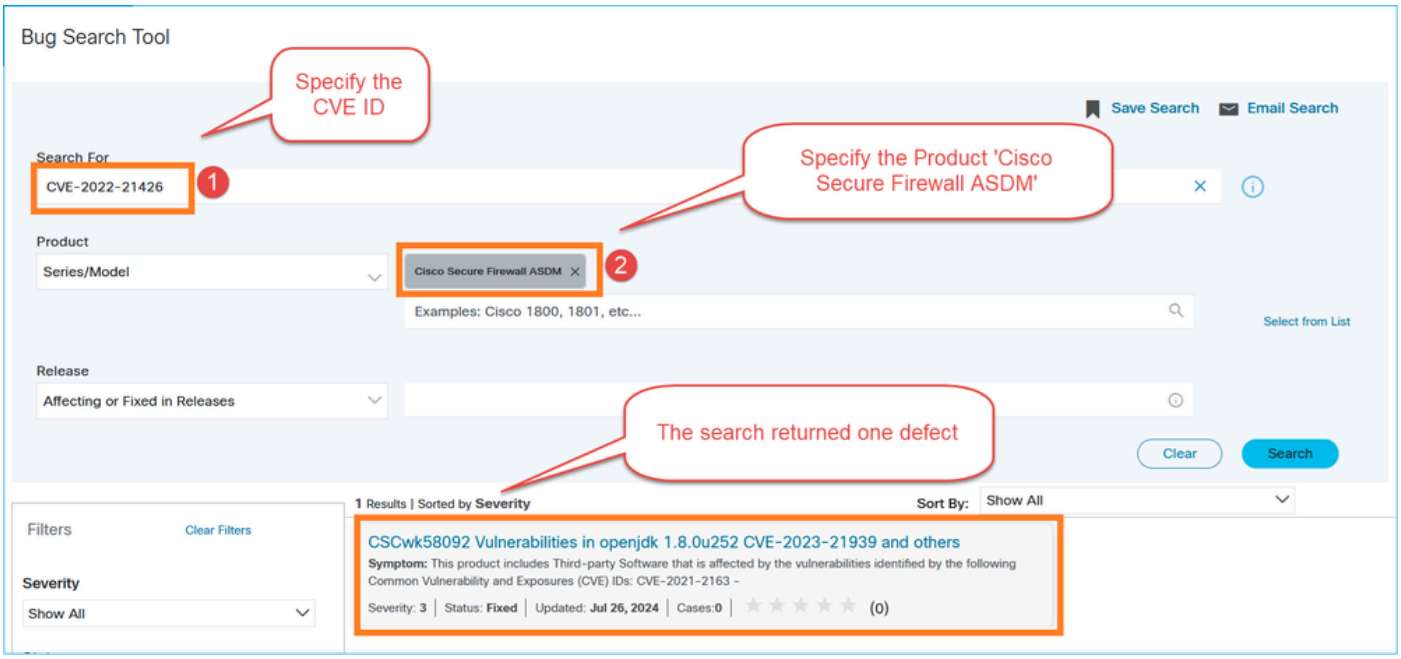


The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

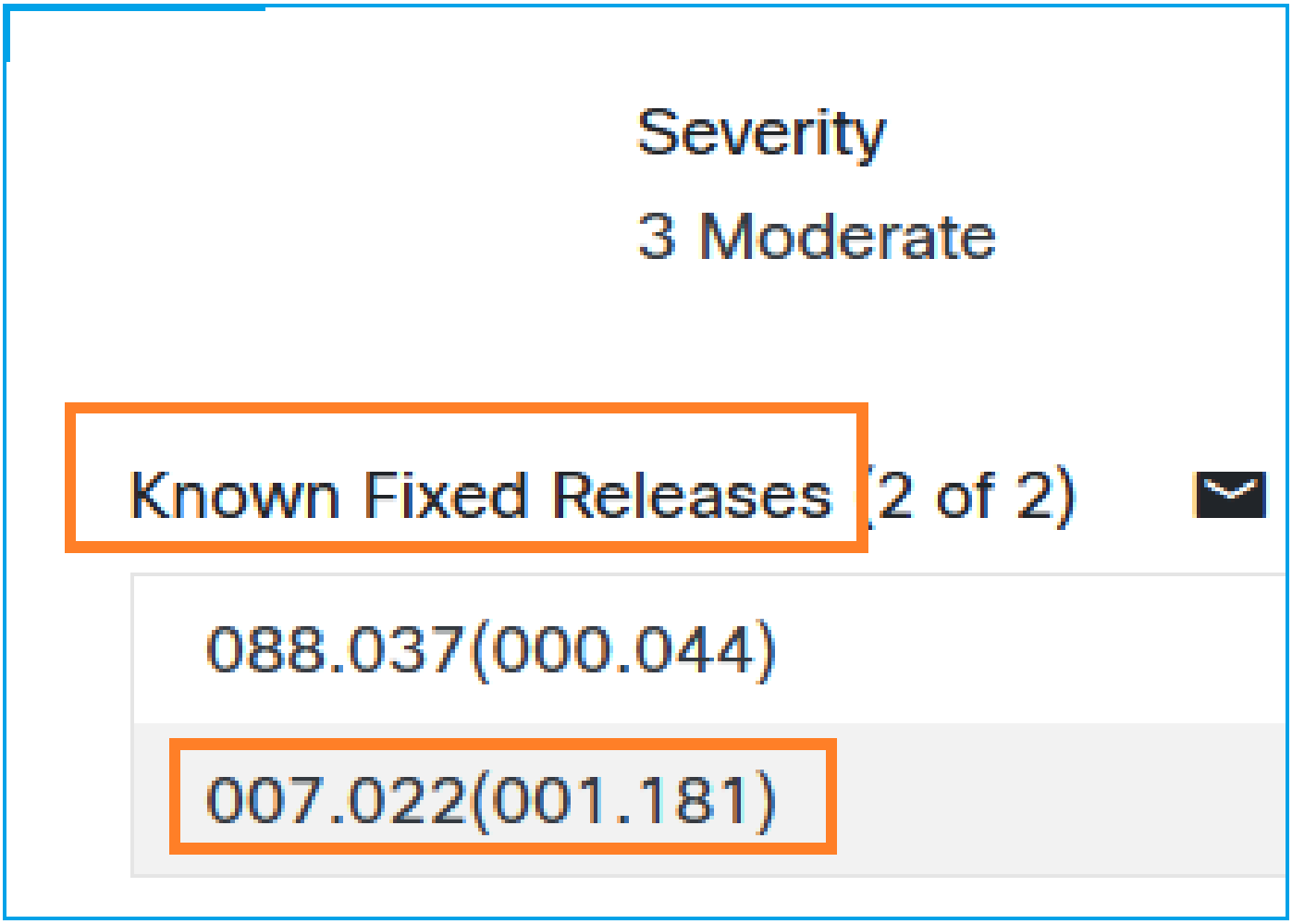
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

Caso não seja encontrado um aviso, pesquise o ID do CVE na Cisco Bug Search Tool (https://bst.cisco.com/bugsearch)





Nesse caso, foi identificado um defeito. Clique nele e verifique seus detalhes e a seção ‘Versões fixas conhecidas’:



O defeito foi corrigido na versão 7.22.1.181 do software ASDM.

Se as pesquisas na ferramenta de consultoria e na ferramenta de pesquisa de bugs para o ID do

CVE especificado não retornarem nada, você precisará trabalhar com o Cisco TAC para esclarecer se o ASDM é afetado pelo CVE.

Referências

- Guias de configuração do ASDM
- Compatibilidade do Cisco ASA e ASDM por modelo

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.