Problemen met ASDM TLS-beveiliging, certificaten en kwetsbaarheid oplossen

Inhoud

Inleiding

Dit document beschrijft het probleemoplossingsproces voor ASDM Transport Layer Security (TLS)-problemen met beveiliging, certificaten en kwetsbaarheden.

Achtergrond

Het document maakt samen met deze documenten deel uit van de serie probleemoplossing voor Adaptieve security applicatie Apparaatbeheer (ASDM):

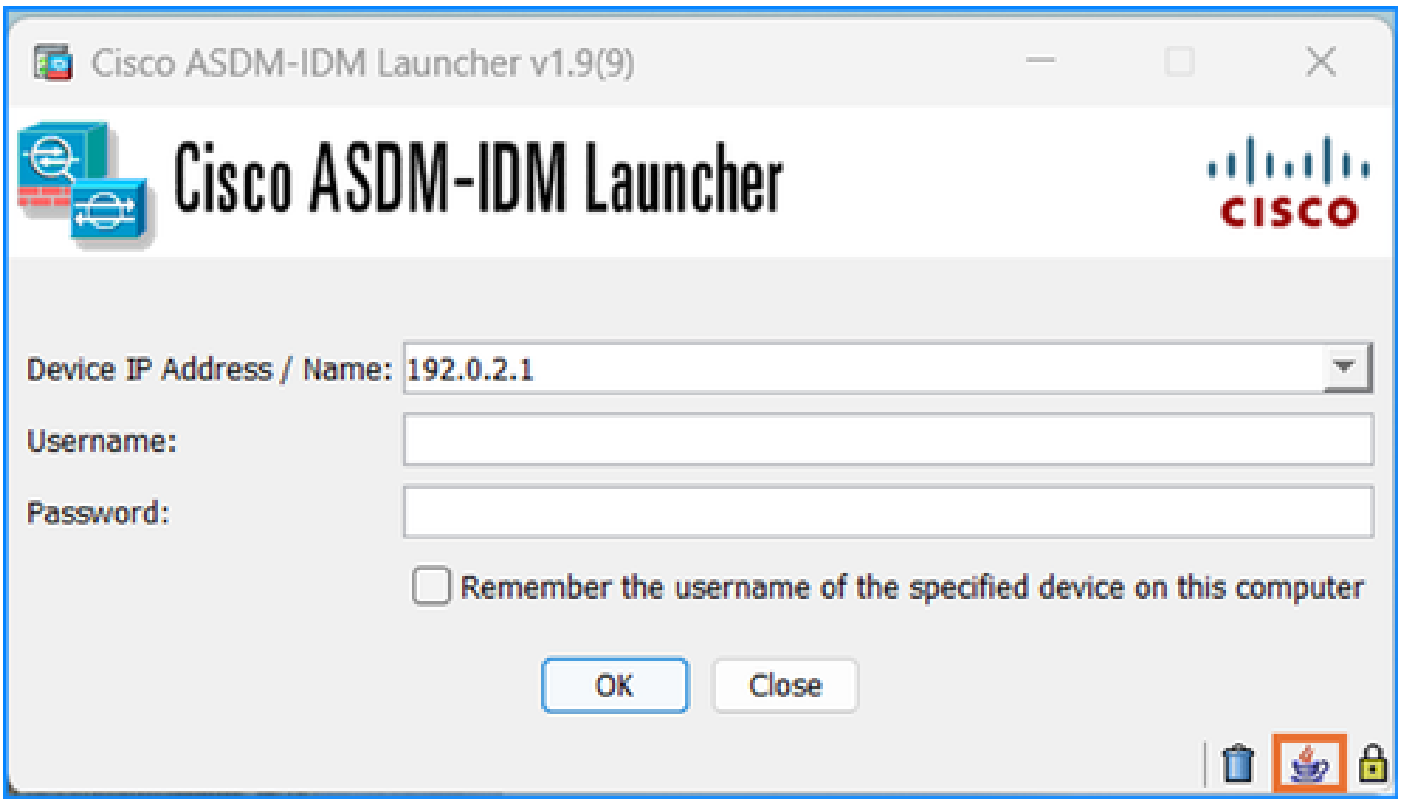
- Problemen met ASDM-start oplossen
- Problemen met ASDM-configuratie, -verificatie en andere problemen oplossen
- Problemen met ASDM-licentie, -upgrade en -compatibiliteit oplossen

Problemen met ASDM TLS-codering

Probleem 1. ASDM kan geen verbinding met de firewall maken vanwege problemen met het TLS-algoritme

ASDM kan geen verbinding maken met de firewall. Een of meer van deze symptomen worden waargenomen:

- ASDM toont het "Kan apparaat niet openen" of de "Kan apparaatbeheer niet starten vanaf <ip>" foutmeldingen.
- De output van de opdracht ssl error bevat de "SSL lib error. Functie: ssl3_get_client_hello Reden: geen gedeeld algoritme"-bericht.
- De Java console logboeken tonen de "javax.net.ssl.SSLHandshakeException: Fataal alarm ontvangen: foutbericht 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)
```

Probleemoplossing - Aanbevolen acties

Een veel voorkomende oorzaak van de symptomen is het mislukken van de TLS-algoritme voor

onderhandeling tussen de ASDM en ASA. In deze gevallen moet de gebruiker, afhankelijk van de configuratie van het algoritme, het certificaat aanpassen aan de ASMD- en/of ASA-kant.

Voer een of meer van deze stappen uit totdat de verbinding succesvol is:

1. In het geval van ASDM met OpenJRE als er sterke TLS-algoritmes worden gebruikt, pas de tijdelijke oplossing van de software toe CSCv12542 Cisco bug ID "ASDM open JRE moet standaard hogere algoritmen gebruiken":
2. Start Kladblok (uitgevoerd als beheerder)
3. Opent het bestand: C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security
4. Zoeken naar: crypto.policy=unlimited
5. Verwijder # voor die regel, zodat alle coderingsopties beschikbaar zijn
6. Opslaan

2. Wijzig de TLS-algoritme-suites op de 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
```

De algoritmeopties voor TLSv1.2:

<#root>

```
ASA(config)#
```

ssl cipher tlsv1.2 ?

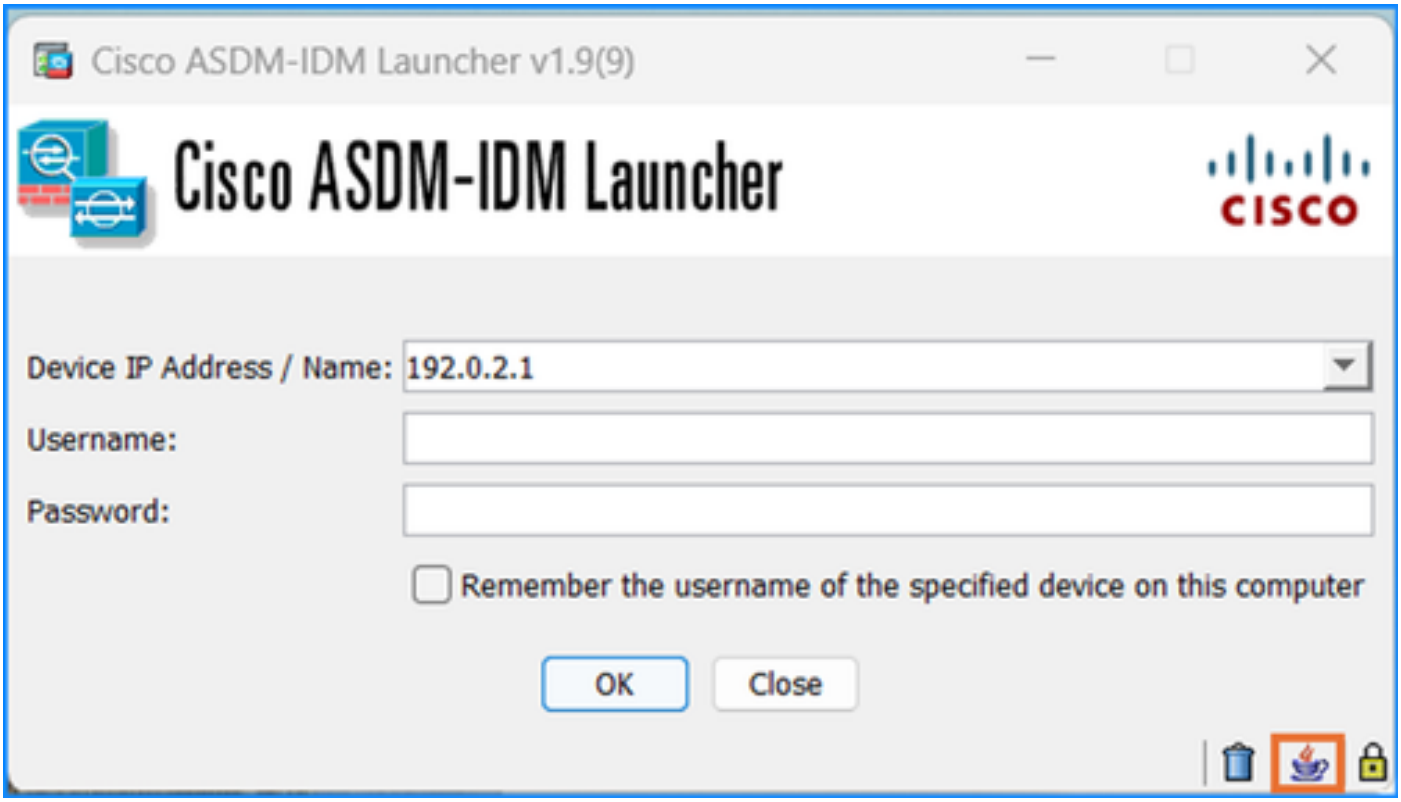
```
configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration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

Waarschuwing: De wijzigingen in de opdracht ssl algoritme worden toegepast op de gehele firewall, inclusief de site-to-site of externe VPN-verbindingen.

Probleem 2. ASDM kan geen verbinding maken met TLS1.3 handshake-fout

De ASDM kan geen verbinding maken met TLS1.3-handshake bij een storing.

De Java console logboeken tonen de "java.lang.IllegalArgumentException: Foutmelding 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)
```

Probleemoplossing - Aanbevolen acties

TLS 1.3-versie moet worden ondersteund op zowel ASA als ASDM. TLS versie 1.3 wordt ondersteund in ASA versies 9.19.1 en hoger (Releaseopmerkingen voor de Cisco Secure Firewall ASA Series, 9.19(x)). De Oracle Java versie 8u261 of hoger is vereist voor ondersteuning van TLS versie 1.3 (Releaseopmerkingen voor Cisco Secure Firewall ASDM, 7.19(x)).

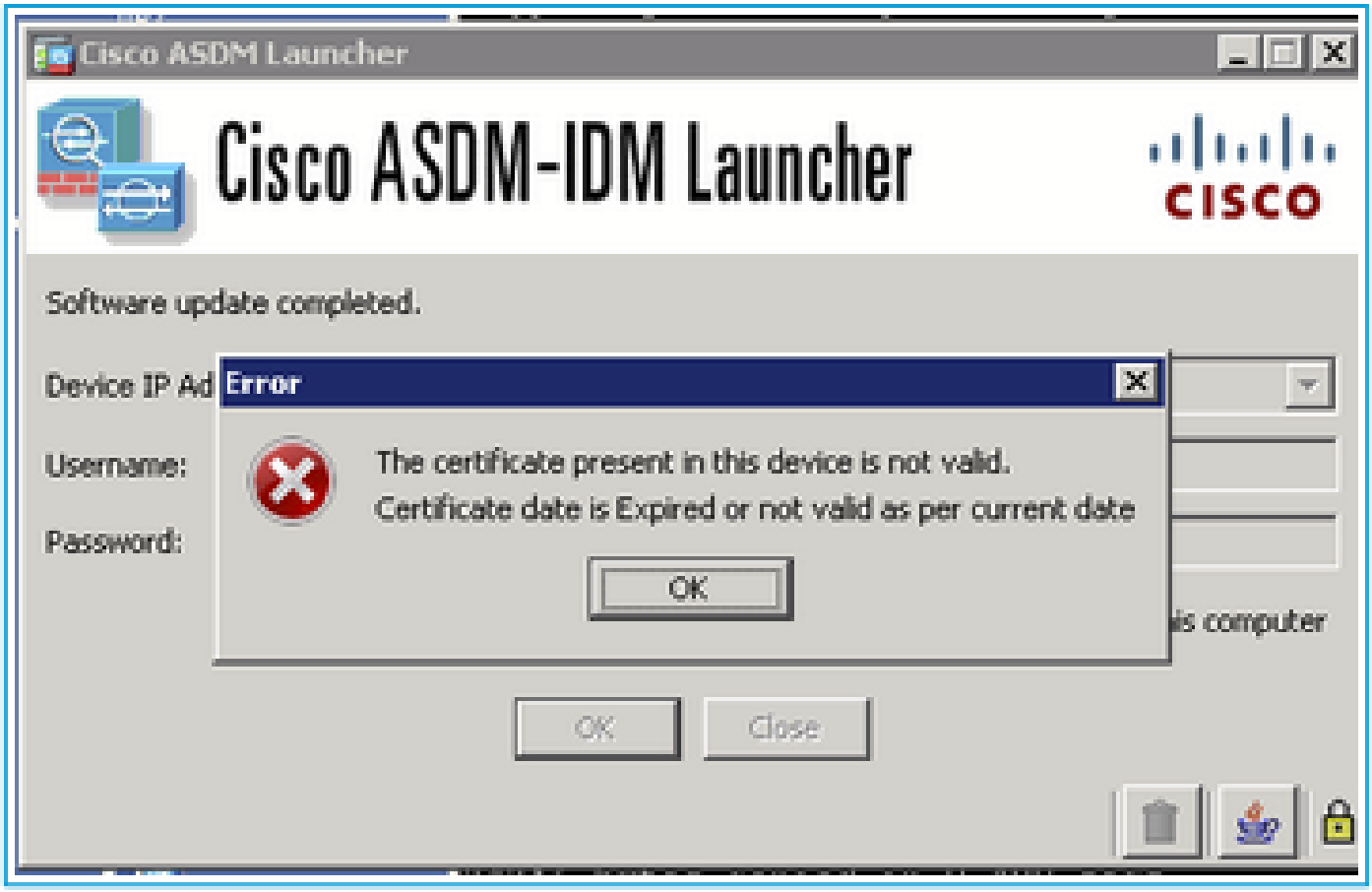
Referenties

1. Releaseopmerkingen voor Cisco Secure Firewall ASA Series, 9.19(x)
2. Releaseopmerkingen voor Cisco Secure Firewall ASDM, 7.19(x)

Problemen met ASDM-certificaten

Probleem 1. "Het certificaat in dit apparaat is ongeldig. De certificaatdatum is verlopen of is niet geldig per huidige datum." (Het stuurprogramma van de VPN-client heeft een fout aangetroffen.) getoond

De foutmelding wordt weergegeven bij het uitvoeren van ASDM: "Het certificaat in dit apparaat is ongeldig. De certificaatdatum is verlopen of is niet geldig per huidige datum."



Soortgelijke symptomen worden beschreven in de opmerkingen bij de afgifte:

"Het zelfondertekende certificaat van ASDM is niet geldig vanwege een tijd- en datumverschil met ASA. ASDM valideert het zelfondertekende SSL-certificaat en als de datum van de ASA niet valt onder de datum van het certificaat Uitgegeven op en Verloopt op datum, zal ASDM niet starten. Zie ASDM-compatibiliteitsopmerkingen

Probleemoplossing - Aanbevolen acties

1. Verlopen certificaten controleren en bevestigen:

<#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. In de ASA Command Line Interface (CLI) verwijdert u het Line Ssl trust-point <cert> <interface>, waarbij de <interface> de naam is die voor ASDM-verbindingen wordt gebruikt. ASA gebruikt een zelfondertekend certificaat voor ASDM-verbindingen.
2. Als er geen zelf-ondertekend certificaat is, produceer één. In dit voorbeeld wordt de ZELF-ondertekende naam gebruikt als een echte puntnaam:

<#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. Koppel het gegenereerde certificaat aan de interface:

<#root>

ssl trust-point SELF-SIGNED

4. Controleer het certificaat:

<#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. Controleer de koppeling van het certificaat aan de interface:

<#root>

```
#
 show run all ssl
```

Probleem 2. Hoe installeert of vernieuwt u certificaten met de ASDM of ASA CLI?

De gebruikers willen de stappen verduidelijken om certificaten te installeren of te vernieuwen met behulp van de ASDM of ASA CLI.

Aanbevolen acties

Raadpleeg de handleidingen voor het installeren en vernieuwen van certificaten:

- ASA: Digitaal certificaat (SSL) installeren en verlengen
- Certificaten installeren en verlengen op ASA, beheerd door CLI

ASDM-kwetsbaarheidsproblemen

In dit gedeelte worden de meest voorkomende problemen in verband met ASDM-kwetsbaarheid besproken.

Probleem 1. Kwetsbaarheid gedetecteerd op ASDM

Als u een kwetsbaarheid op ASDM detecteert.

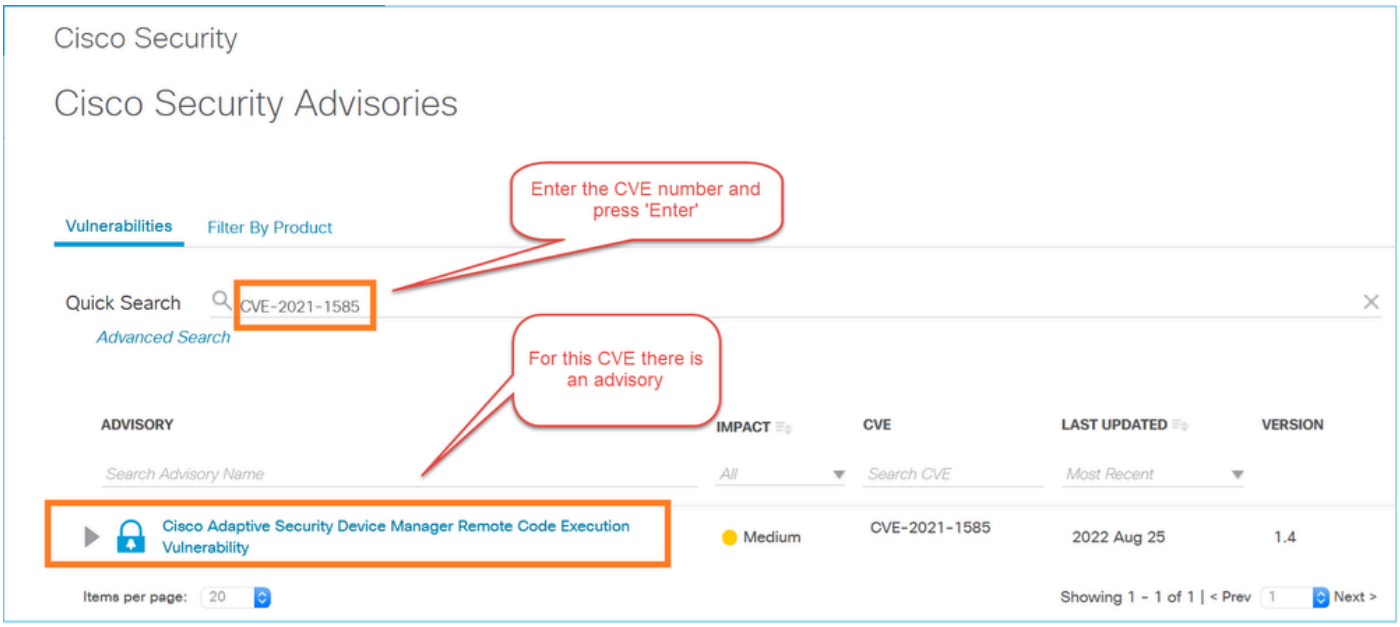
Probleemoplossing - Aanbevolen stappen

Stap 1: Identificeer de CVE-id (bijvoorbeeld CVE-2023-21930)

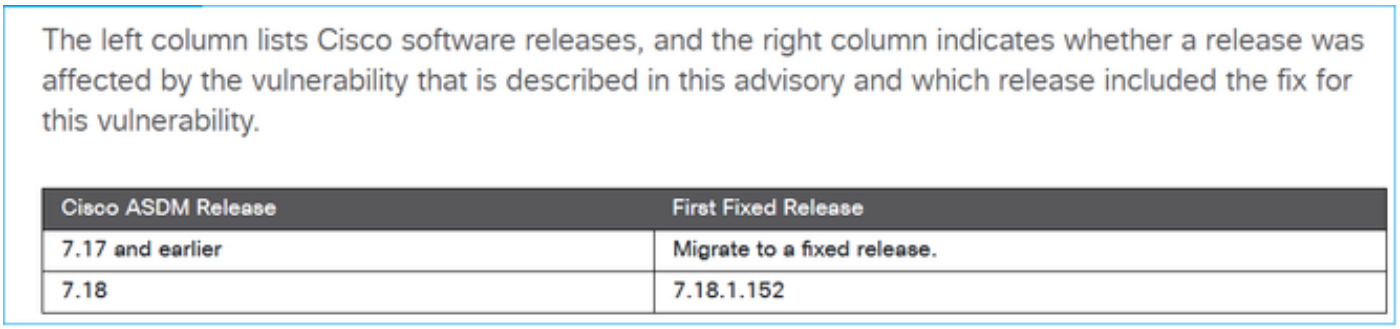
Stap 2: Zoeken naar CVE in Cisco Security Advisories en Cisco Bug Search Tool:

Naar de adviespagina navigeren:

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



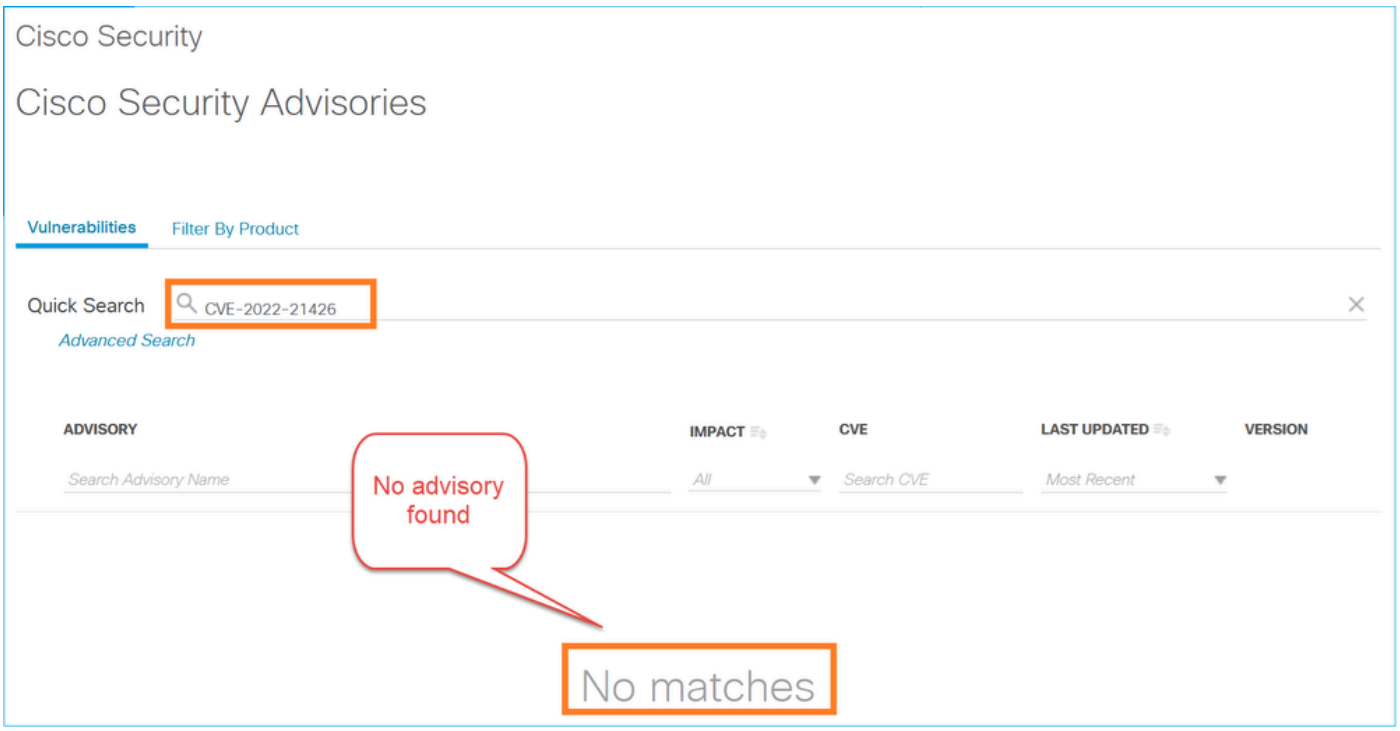
Open het advies en controleer als ASDM wordt beïnvloed, bijvoorbeeld:

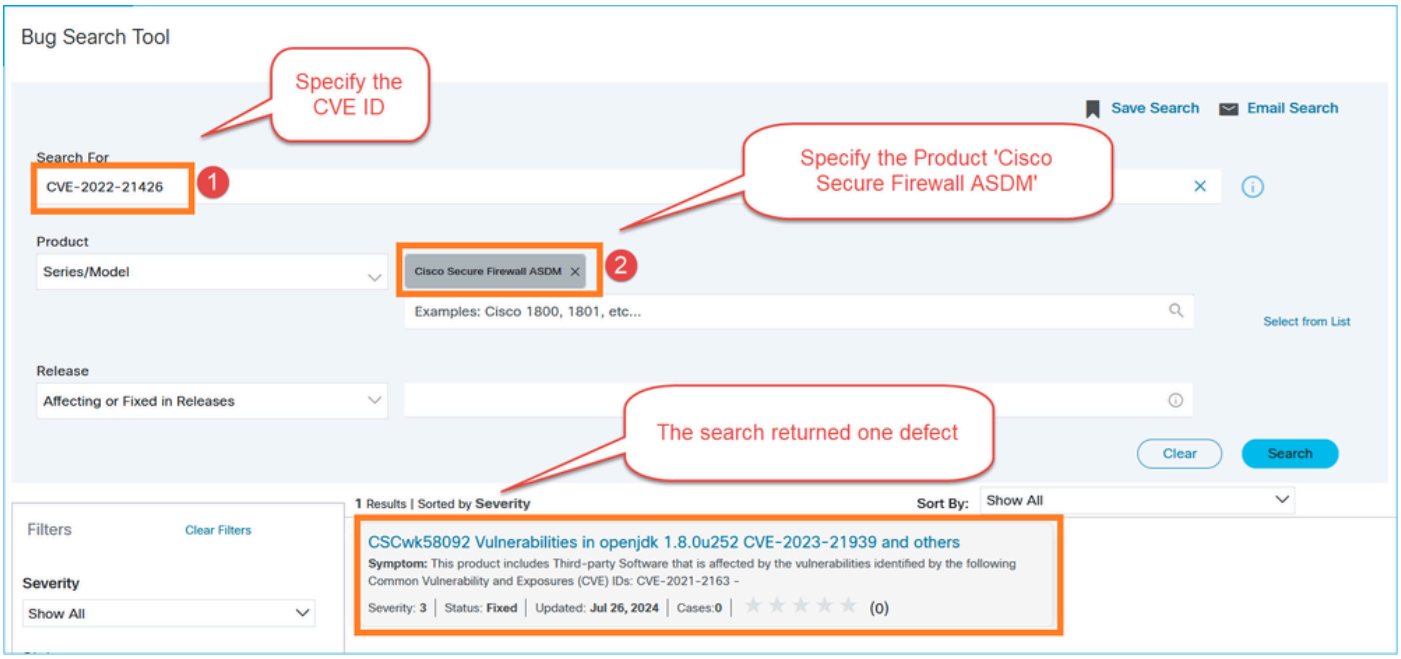


The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

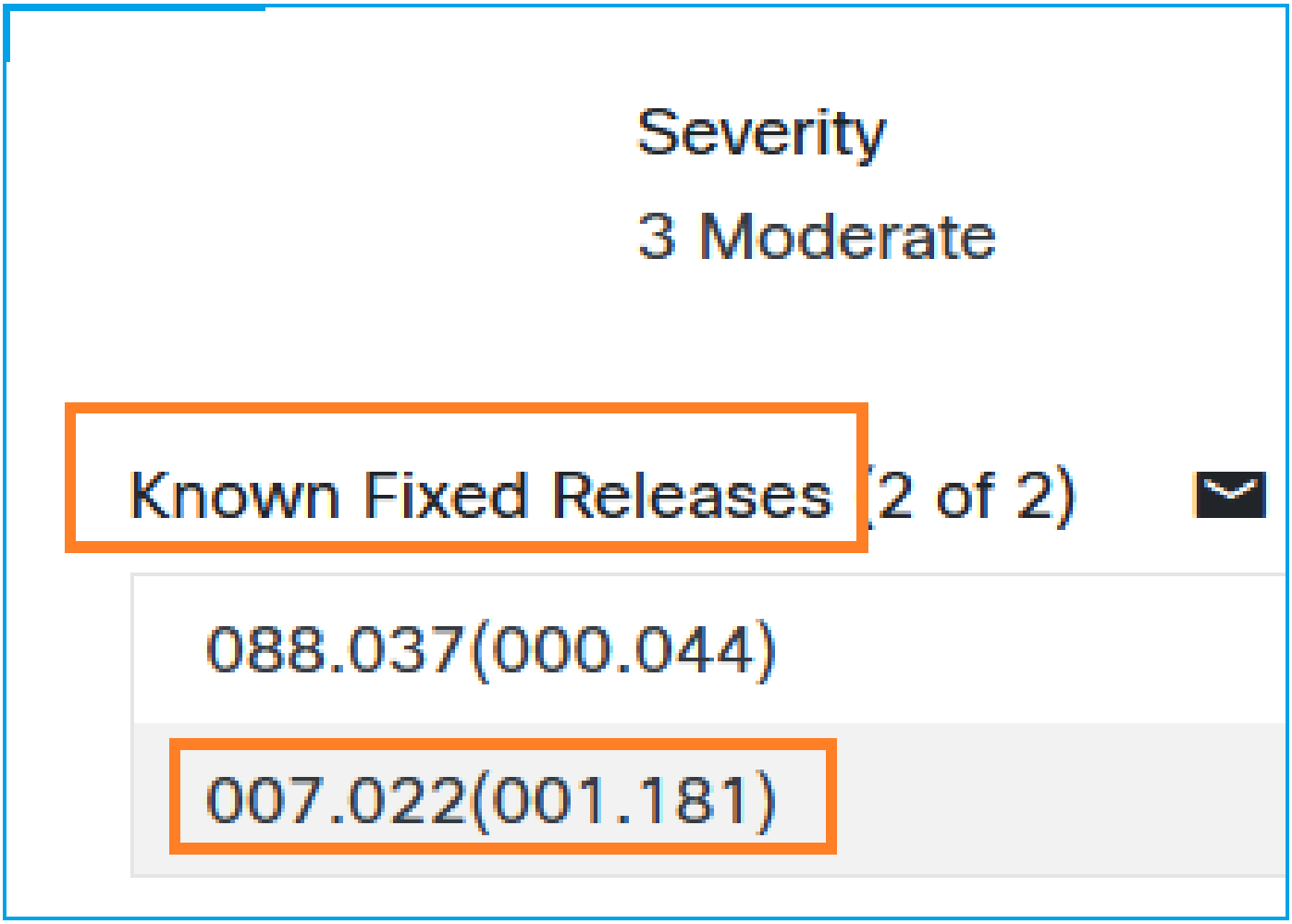
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

Als u geen advies hebt gevonden, zoekt u naar de CVE-id in de Cisco Bug Search Tool (https://bst.cisco.com/bugsearch)





In dit geval werd een defect vastgesteld. Klik erop en controleer de gegevens en de sectie ‘Bekende vaste releases’:



Het defect is verholpen in 7.22.1.181 ASDM-softwarerelease.

Als de zoekopdrachten in de adviserende tool en bug search tool voor de gespecificeerde CVE ID

niets teruggaven, moet u werken met Cisco TAC om te verduidelijken als ASDM wordt beïnvloed door de CVE.

Referenties

- ASDM-configuratiehandleidingen
- Cisco ASA- en ASDM-compatibiliteit per model

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.