Fehlerbehebung bei ASDM TLS-Sicherheits-, Zertifikat- und Schwachstellenproblemen

Inhalt

Einleitung

In diesem Dokument wird der Fehlerbehebungsprozess für ASDM Transport Layer Security (TLS)-Sicherheits-, Zertifikat- und Schwachstellenprobleme beschrieben.

Hintergrund

Das Dokument ist zusammen mit den folgenden Dokumenten Teil der ASDM-Reihe (Adaptive Security Appliance Device Manager) zur Fehlerbehebung:

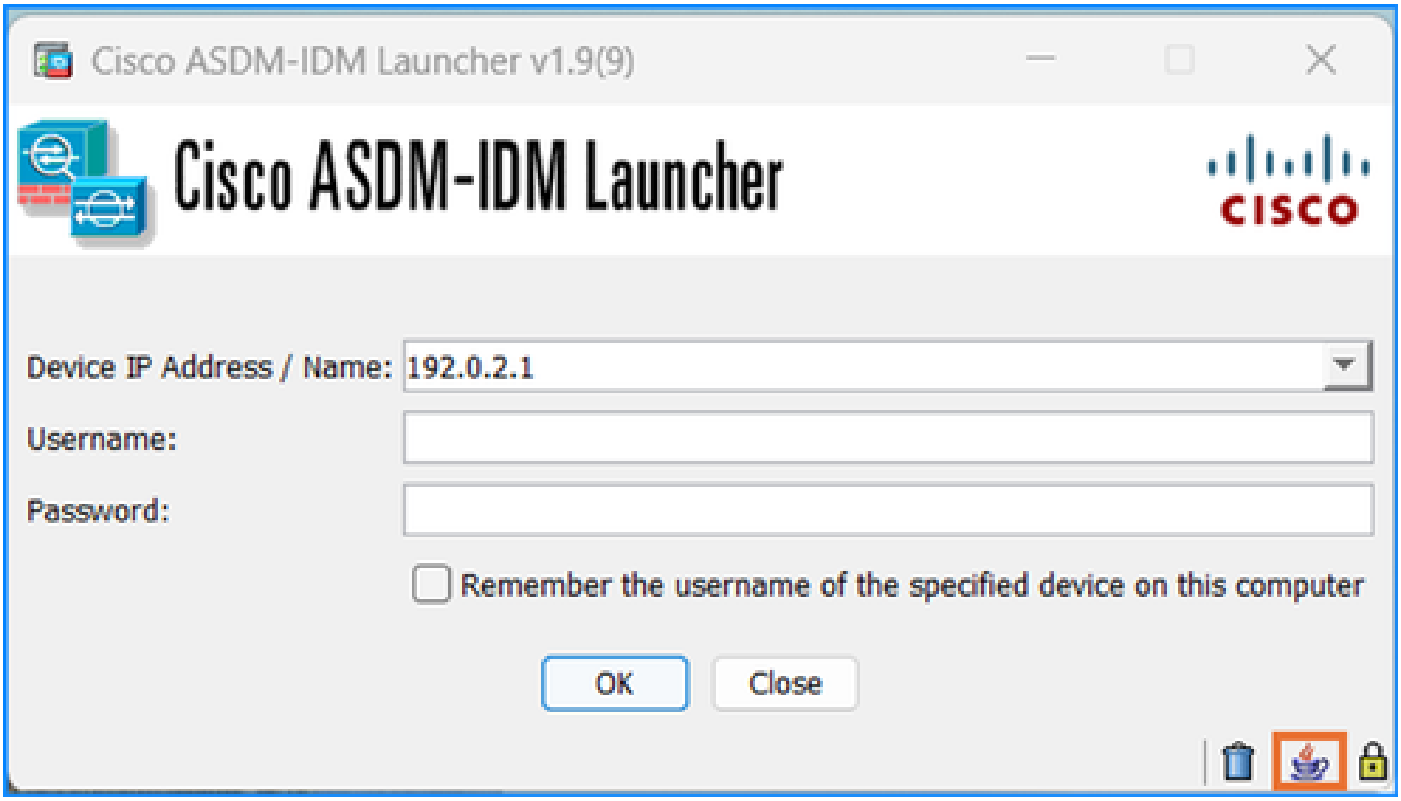
- Fehlerbehebung bei ASDM-Startproblemen
- Fehlerbehebung bei ASDM-Konfiguration, Authentifizierung und anderen Problemen
- Fehlerbehebung bei ASDM-Lizenz-, Upgrade- und Kompatibilitätsproblemen

ASDM TLS-Verschlüsselungsprobleme

Problem 1: ASDM kann aufgrund von TLS-Verschlüsselungsproblemen keine Verbindung zur Firewall herstellen

ASDM kann keine Verbindung zur Firewall herstellen. Eines oder mehrere der folgenden Symptome wurden beobachtet:

- ASDM zeigt die Fehlermeldungen "Konnte Gerät nicht öffnen" oder "Gerätemanager kann nicht von <ip> gestartet werden".
- Die Ausgabe des Befehls show ssl error enthält den Fehler "SSL lib. Funktion: ssl3_get_client_hello Grund: "no shared cipher".
- In den Java-Konsolenprotokollen wird die folgende Meldung angezeigt: "javax.net.ssl.SSLHandshakeException: Erhaltene schwerwiegende Warnung: handshake_failure" Fehlermeldung:



<#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)
```

Fehlerbehebung - empfohlene Maßnahmen

Eine häufige Ursache der Symptome ist der Fehler bei der TLS-Verschlüsselungssuite-Aushandlung zwischen dem ASDM und der ASA. In diesen Fällen muss der Benutzer das Zertifikat auf ASMD- und/oder ASA-Seite je nach Verschlüsselungskonfiguration anpassen.

Führen Sie einen oder mehrere der folgenden Schritte durch, bis die Verbindung erfolgreich hergestellt wurde:

1. Im Fall von ASDM mit OpenJRE, wenn starke TLS-Verschlüsselungs-Suites verwendet werden, wenden Sie die Problemumgehung aus der Software an Cisco Bug-ID CSCv12542 "ASDM open JRE should use higher ciphers by default":
2. Starten Sie den Editor (führen Sie ihn als Administrator aus)
3. Datei öffnen: C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security
4. Suche nach: crypto.policy=unbegrenzt
5. Entfernen Sie # vor dieser Zeile, damit alle Verschlüsselungsoptionen verfügbar sind.
6. Speichern

2. Ändern Sie die TLS-Verschlüsselungssuiten auf der 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
```

Die Verschlüsselungsoptionen für TLSv1.2:

<#root>

```
ASA(config)#
```

ssl cipher tlsv1.2 ?

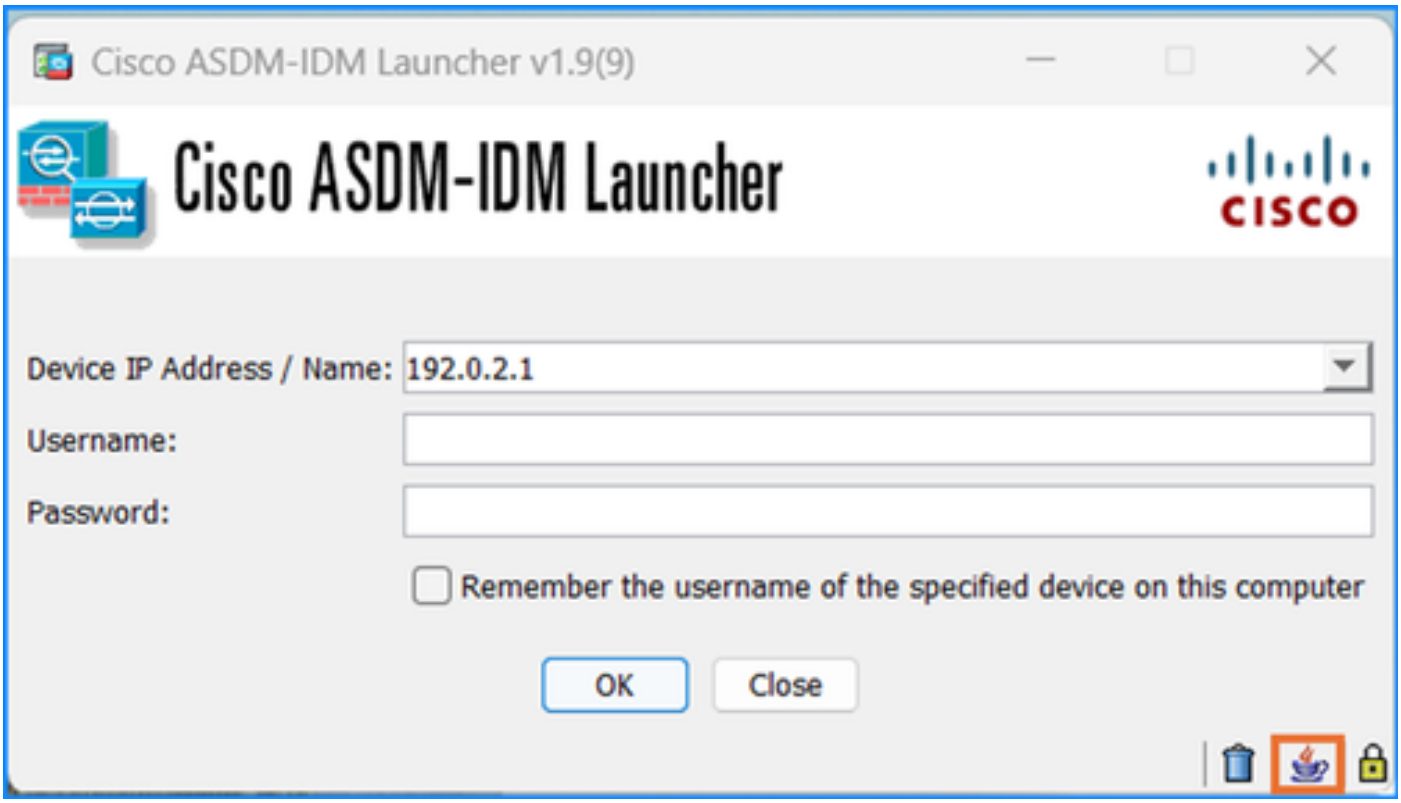
```
configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration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

⚠ Warnung: Die Änderungen im ssl-Verschlüsselungsbefehl werden auf die gesamte Firewall angewendet, einschließlich der Site-to-Site- oder Remote-Access-VPN-Verbindungen.

Problem 2: ASDM kann aufgrund eines TLS1.3-Handshake-Fehlers keine Verbindung mit herstellen

Der ASDM kann aufgrund eines TLS1.3-Handshake-Fehlers keine Verbindung mit herstellen.

Die Java-Konsolenprotokolle zeigen die "java.lang.IllegalArgumentException: TLSv1.3"-Fehlermeldung:



<#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)
```

Fehlerbehebung - empfohlene Maßnahmen

Die TLS 1.3-Version muss sowohl auf ASA als auch auf ASDM unterstützt werden. TLS-Version 1.3 wird von ASA-Versionen 9.19.1 und höher unterstützt (Versionshinweise für die Cisco Secure

Firewall ASA-Serie, 9.19(x)). Die Oracle Java-Version 8u261 oder höher ist für die Unterstützung von TLS-Version 1.3 (Release Notes for Cisco Secure Firewall ASDM, 7.19(x)) erforderlich.

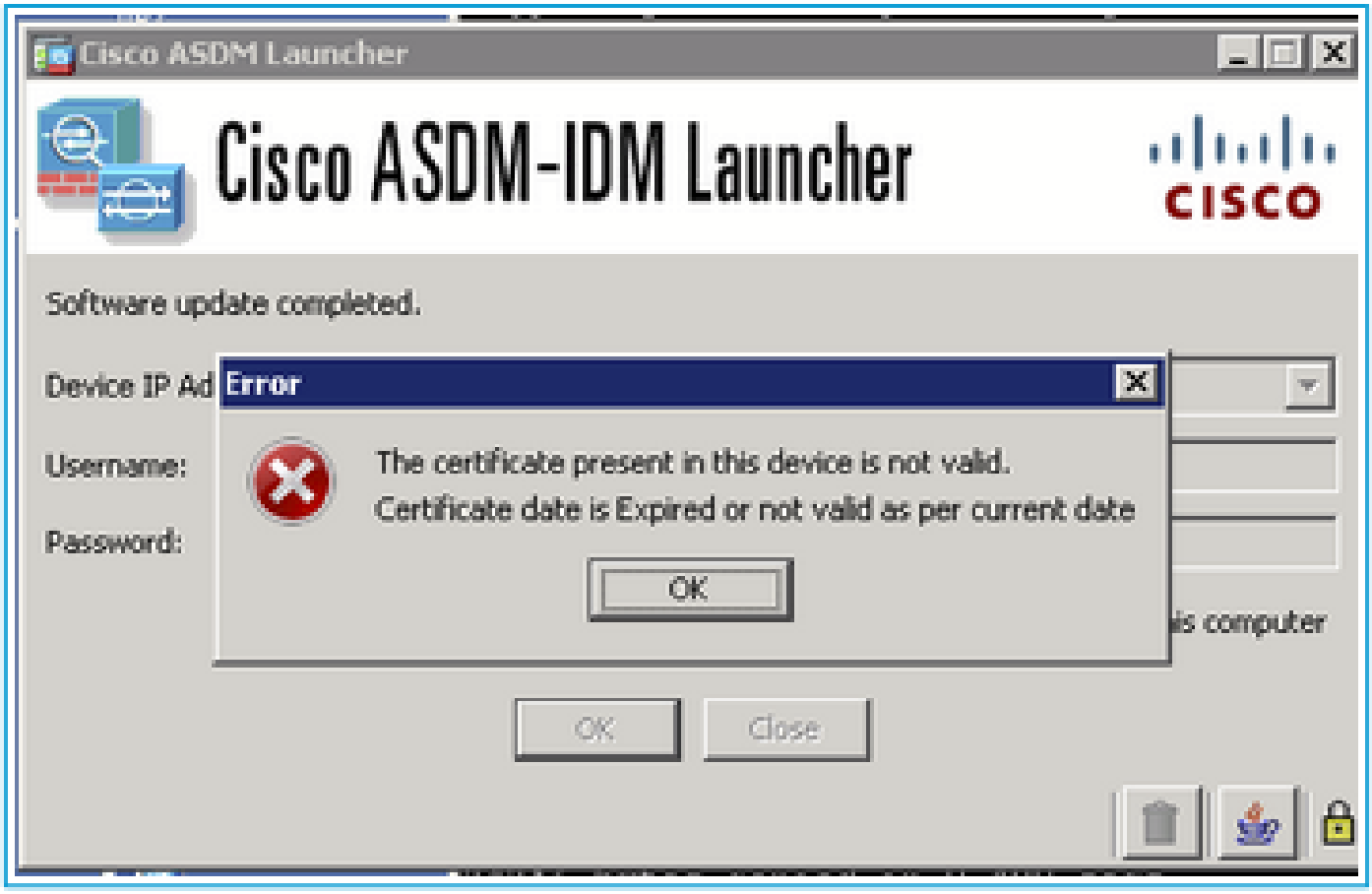
Referenzen

1. Versionshinweise für die Cisco Secure Firewall ASA-Serie, 9.19(x)
2. Versionshinweise für Cisco Secure Firewall ASDM, 7.19(x)

ASDM-Zertifikatprobleme

Problem 1. "Das in diesem Gerät vorhandene Zertifikat ist ungültig. Das Zertifikatsdatum ist abgelaufen oder nicht als aktuelles Datum gültig." fehl

Bei der Ausführung von ASDM wird folgende Fehlermeldung angezeigt: "Das in diesem Gerät vorhandene Zertifikat ist ungültig. Das Zertifikatsdatum ist abgelaufen oder nicht als aktuelles Datum gültig."



Ähnliche Symptome werden in den Versionshinweisen beschrieben:

"Das selbstsignierte ASDM-Zertifikat ist ungültig, da Uhrzeit und Datum nicht mit der ASA übereinstimmen. ASDM validiert das selbstsignierte SSL-Zertifikat. Wenn das Datum der ASA

nicht dem Datum für Ausgestellt am und Ablauf am entspricht, wird ASDM nicht gestartet. Siehe [ASDM-Kompatibilitätshinweise]

Fehlerbehebung - empfohlene Maßnahmen

1. Überprüfen und bestätigen Sie abgelaufene Zertifikate:

<#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. Entfernen Sie in der ASA Command Line Interface (CLI) die Zeile ssl trust-point <cert> <interface>, wobei die <Schnittstelle> der für ASDM-Verbindungen verwendete Name ist.

Die ASA verwendet selbstsignierte Zertifikate für ASDM-Verbindungen.

2. Wenn es kein selbstsigniertes Zertifikat gibt, generieren Sie es. In diesem Beispiel wird der SELF-SIGNED-Name als echter Punktname verwendet:

<#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. Ordnen Sie das generierte Zertifikat der Schnittstelle zu:

<#root>

ssl trust-point SELF-SIGNED

4. Überprüfen Sie das Zertifikat:

<#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: 29055b2efdd3737c8bb335f578338a3d7831c63
```

5. Überprüfen Sie die Zertifikatzuordnung zur Schnittstelle:

<#root>

#

show run all ssl

Problem 2. Wie werden Zertifikate mit dem ASDM oder der ASA CLI installiert oder erneuert?

Die Benutzer möchten die Schritte zur Installation oder Verlängerung von Zertifikaten mithilfe von ASDM oder ASA CLI erläutern.

Empfohlene Maßnahmen

Informationen zur Installation und Verlängerung von Zertifikaten finden Sie in den folgenden Handbüchern:

- ASA: Installation und Verlängerung digitaler SSL-Zertifikate
- Installieren und Erneuern von Zertifikaten auf von CLI verwalteten ASA

ASDM-Schwachstellenprobleme

In diesem Abschnitt werden die häufigsten ASDM-Schwachstellenprobleme behandelt.

Problem 1. Auf ASDM erkannte Schwachstelle

Falls Sie eine Schwachstelle auf ASDM entdecken.

Fehlerbehebung - Empfohlene Schritte

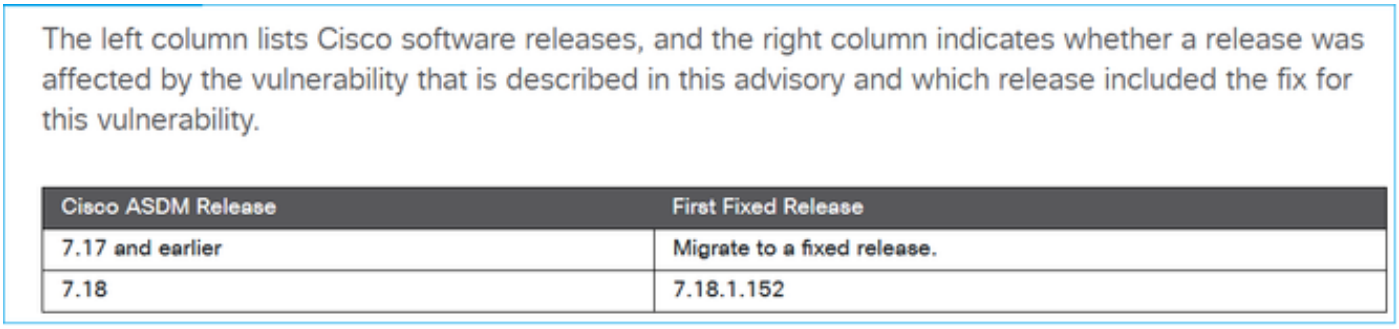
Schritt 1: Geben Sie die CVE-ID an (z. B. CVE-2023-21930).

Phase 2: Suchen Sie im Cisco Security Advisories and Cisco Bug Search Tool nach der CVE:

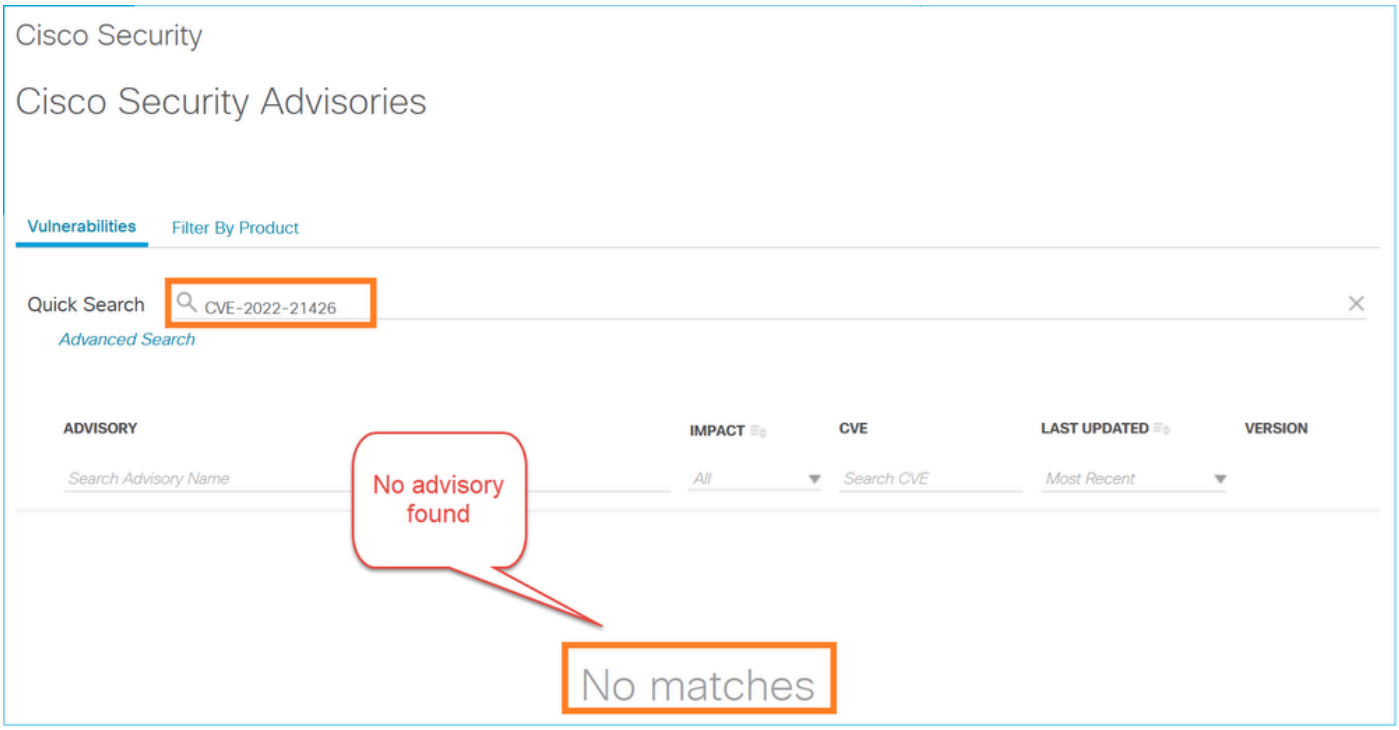
Navigieren Sie zur Seite "Beratung":

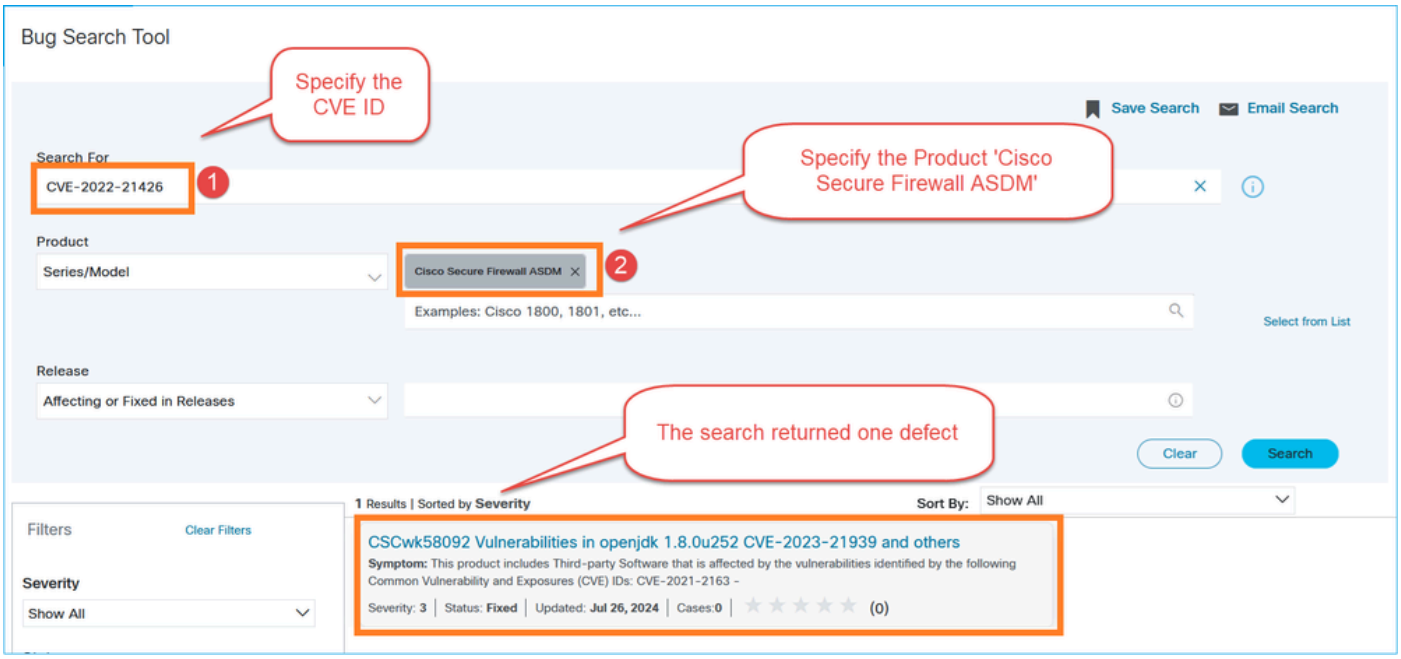
https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Öffnen Sie die Beratung, und überprüfen Sie, ob ASDM betroffen ist. Beispiel:

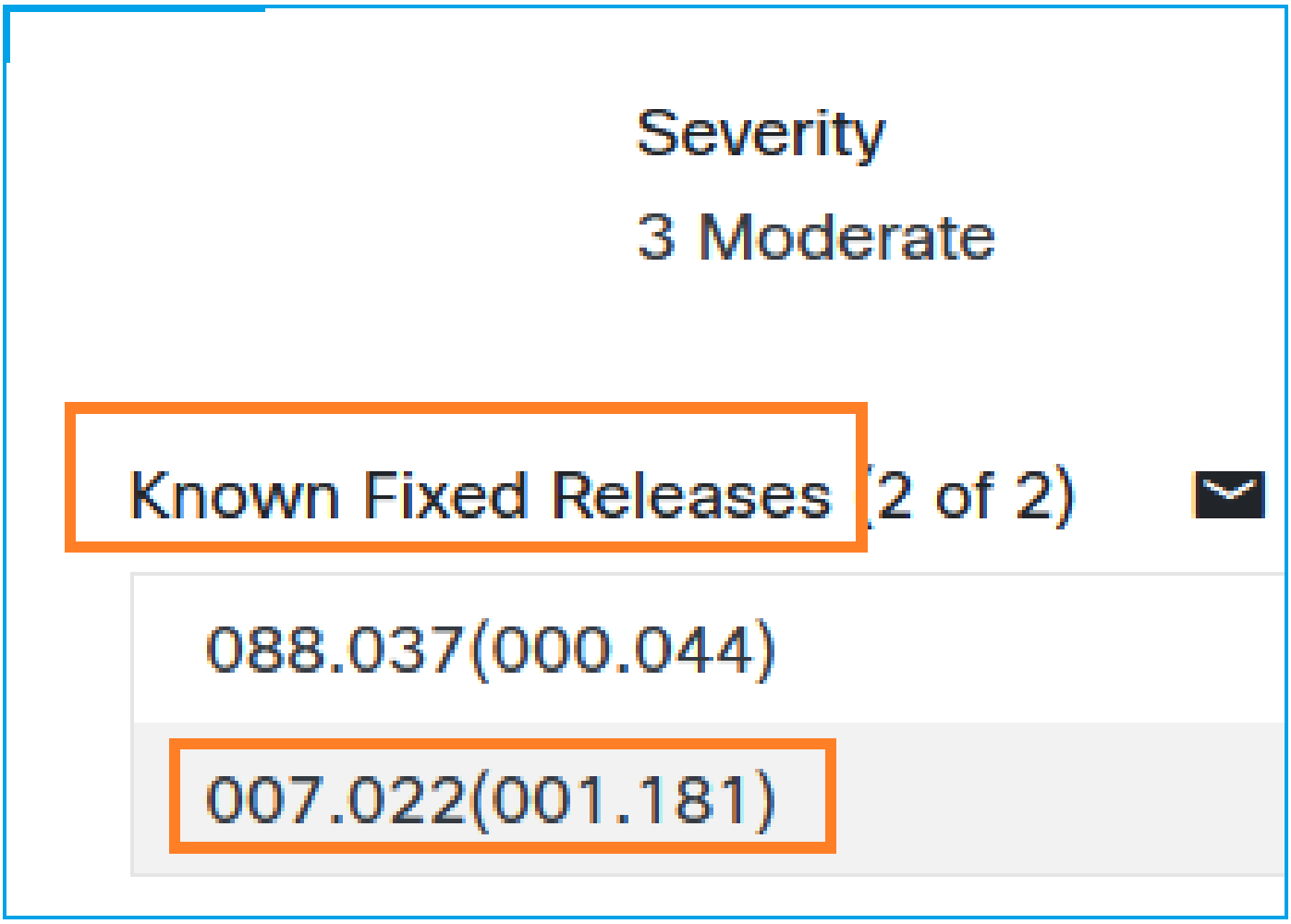


Sollte keine Benachrichtigung gefunden werden, suchen Sie im Cisco Bug Search Tool (https://bst.cisco.com/bugsearch)





In diesem Fall wurde ein Mangel festgestellt. Klicken Sie darauf, und überprüfen Sie die Details sowie den Abschnitt "Known Fixed Releases":



Der Fehler wurde in der ASDM-Softwareversion 7.22.1.181 behoben.

Wenn die Suchergebnisse im Advisory Tool und im Bug Search Tool für die angegebene CVE-ID nichts ergeben haben, müssen Sie zusammen mit dem Cisco TAC klären, ob ASDM von dem CVE betroffen ist.

Referenzen

- ASDM-Konfigurationsanleitungen
- Kompatibilität von Cisco ASA und ASDM pro Modell

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.