ASDM TLSのセキュリティ、証明書、および脆弱性の問題のトラブルシューティング

内容

はじめに

このドキュメントでは、ASDM Transport Layer Security(TLS)セキュリティ、証明書、および脆弱性の問題のトラブルシューティングプロセスについて説明します。

背景

このドキュメントは、Adaptive Security Appliance(ASA)Device Manager(ASDM)のトラブルシューティングシリーズの一部で、次のドキュメントとともに提供されています。

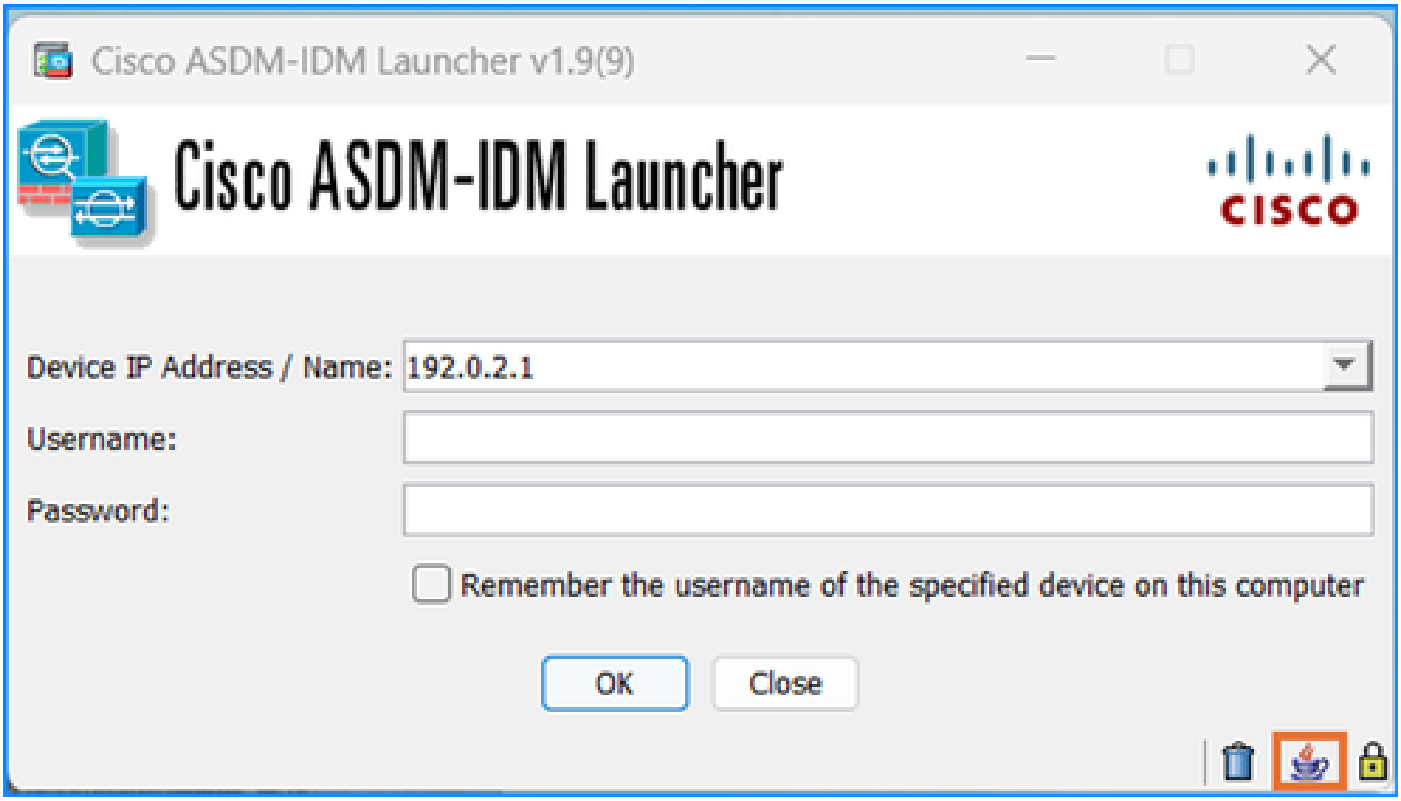
- ASDM起動問題のトラブルシューティング
- ASDMの設定、認証、およびその他の問題のトラブルシューティング
- ASDMライセンス、アップグレード、および互換性の問題のトラブルシューティング

ASDM TLS暗号化の問題

問題1: ASDMがTLS暗号化の問題によりファイアウォールに接続できない

ASDMがファイアウォールに接続できません。次の症状が1つ以上見られます。

- ASDMで「Could not open device」または「Unable to launch device manager from <ip>」エラーメッセージが表示される。
- show ssl errorコマンドの出力に、「SSL lib error.Function: ssl3_get_client_hello Reason: no shared cipher」メッセージを送信します。
- Javaコンソールログに「javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure」というエラーメッセージが表示されます。



<#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)
```

トラブルシューティング – 推奨処置

この症状の一般的な根本原因は、ASDMとASA間のTLS暗号スイートのネゴシエーションの失敗です。この場合、暗号設定に応じて、ユーザはASMD側またはASA側（あるいはその両方）で証明書を調整する必要があります。

接続が成功するまで、次の手順を1つ以上実行します。

1. OpenJREを使用するASDMで強力なTLS暗号スイートが使用されている場合、Cisco Bug ID CSCvv12542「ASDMオープンJREはデフォルトでより高い暗号を使用する必要がある」というソフトウェアからの回避策を適用します。
2. メモ帳を起動する（管理者として実行）
3. ファイルC:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.securityを開きます。
4. 検索：crypto.policy=unlimited
5. その行の前にある#を削除し、すべての暗号化オプションを使用可能にします
6. 保存します。

2. ASAのTLS暗号スイートを変更します。

<#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
```

TLSv1.2の暗号オプション：

<#root>

```
ASA(config)#
```

ssl cipher tlsv1.2 ?

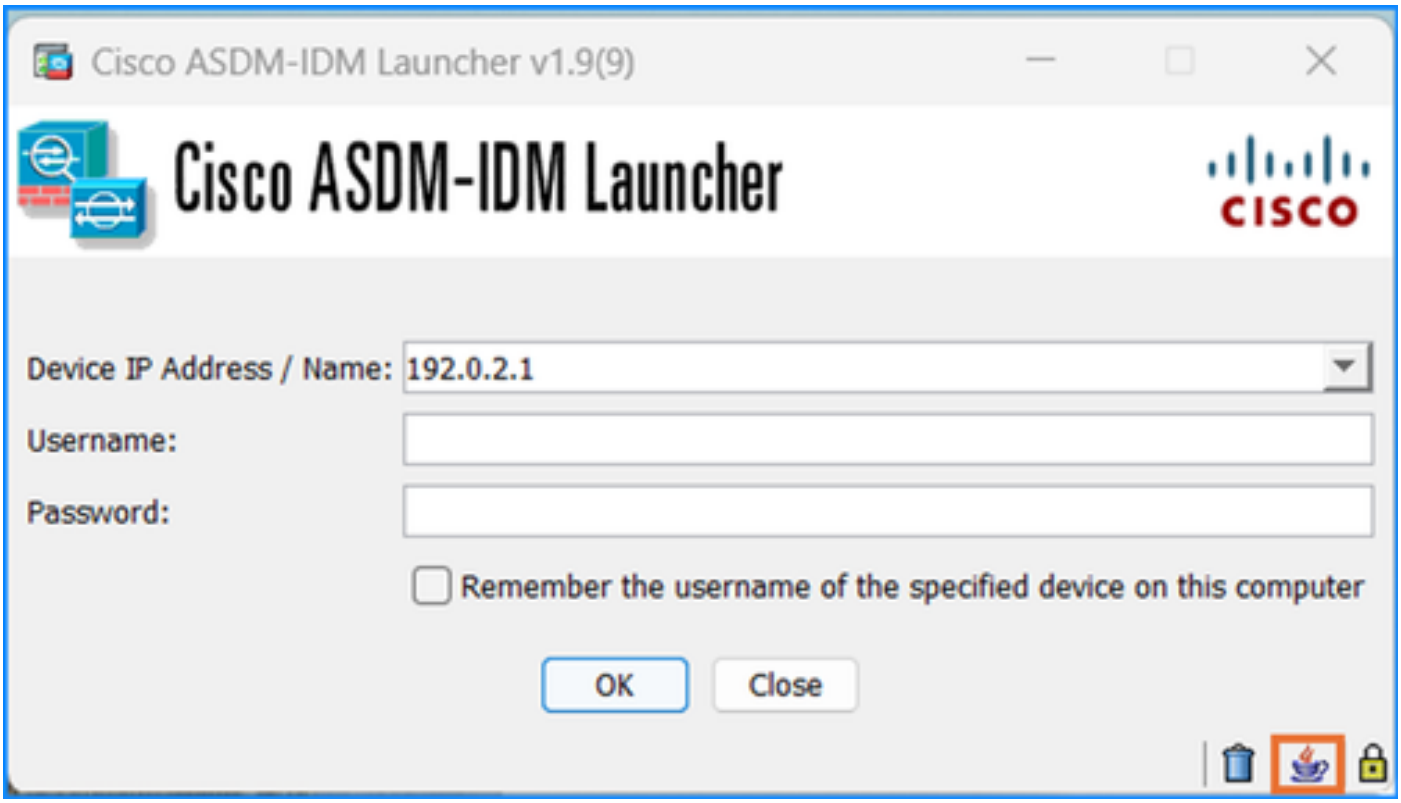
```
configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration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

警告: ssl cipherコマンドでの変更は、サイト間またはリモートアクセスVPN接続を含むファイアウォール全体に適用されます。

問題2. TLS1.3ハンドシェイクの失敗により、ASDMはに接続できない

ASDMは、TLS1.3ハンドシェイクの失敗が原因でに接続できません。

Javaコンソールログに「java.lang.IllegalArgumentException: TLSv1.3」エラーメッセージが表示されます。



<#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)
```

トラブルシューティング – 推奨処置

TLS 1.3バージョンは、ASAとASDMの両方でサポートされている必要があります。TLSバージョン1.3は、ASAバージョン9.19.1以降でサポートされています(Cisco Secure Firewall ASAシリーズ 9.19(x)リリースノート)。TLSバージョン1.3をサポートするには、Oracle Javaバージョン 8u261以降が必要です(Cisco Secure Firewall ASDM 7.19(x)リリースノート)。

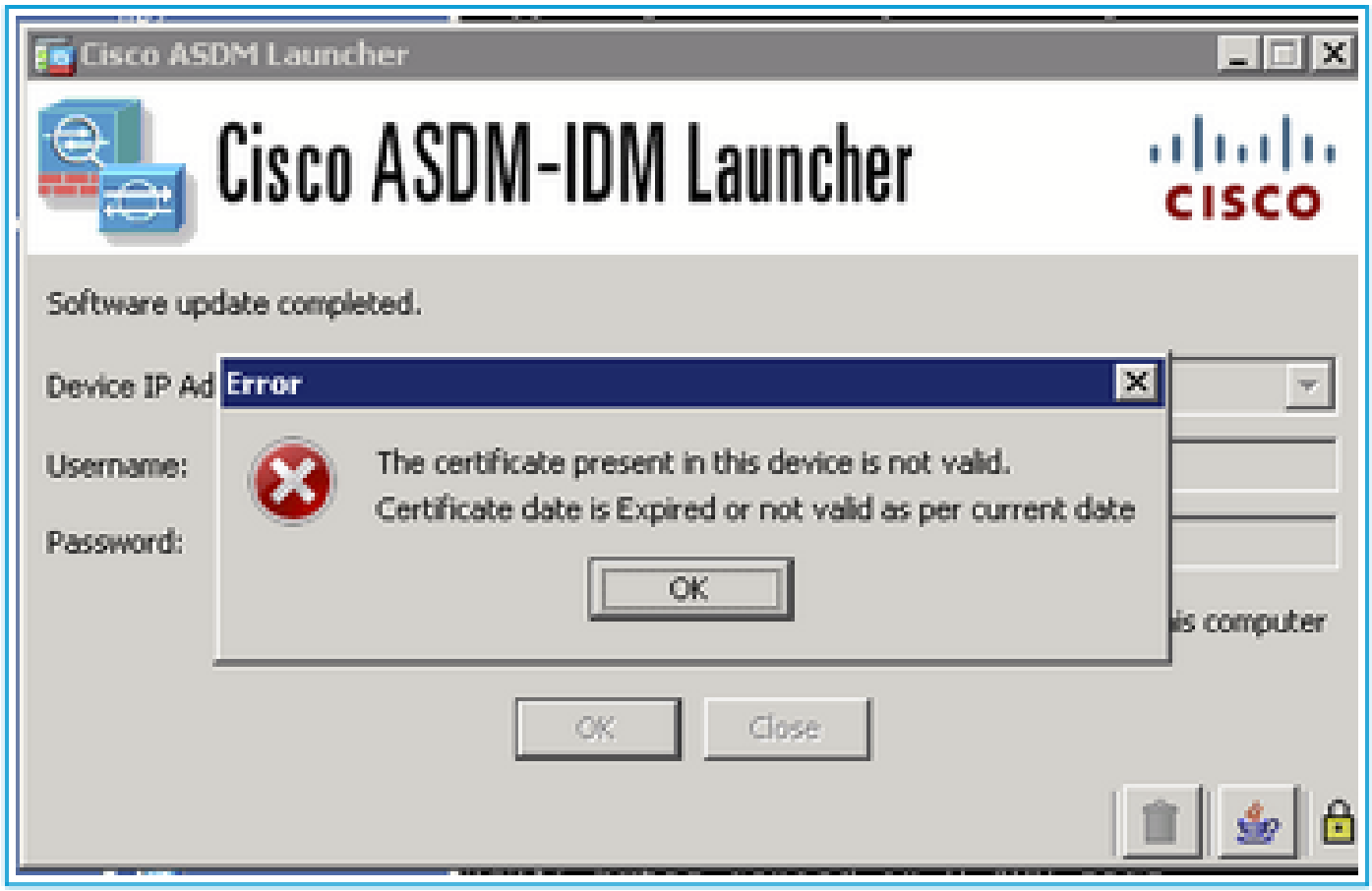
参考資料

1. Cisco Secure Firewall ASAシリーズ9.19(x)リリースノート
2. Cisco Secure Firewall ASDM 7.19(x)リリースノート

ASDM証明書の問題

問題 1.“このデバイスに存在する証明書は無効です。証明書の日付が期限切れであるか、現在の日付では無効です」というエラーメッセージが表示されます。

ASDMを実行すると、「The certificate present in this device is not valid.証明書の有効期限が切れているか、現在の日付では無効です。



同様の症状については、リリースノートで説明しています。

「ASDMの自己署名証明書が、ASAと時刻と日付が一致していないために有効でない：ASDMが自己署名SSL証明書を検証し、ASAの日付が証明書の「発行日」と「有効期限」の間にない場合、ASDMは起動しません。次を参照してください。 ASDMの互換性に関する注意事項

トラブルシューティング – 推奨処置

1. 期限切れの証明書を確認します。

```
<#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. ASAコマンドラインインターフェイス(CLI)で、ssl trust-point <cert> <interface>の行を削除します。ここで、<interface>はASDM接続に使用されるnameifです。ASAはASDM接続に自己署名証明書を使用します。
2. 自己署名証明書がない場合は、証明書を生成します。次の例では、SELF-SIGNEDという名前が実際のポイント名として使用されています。

```
<#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. 生成された証明書をインターフェイスに関連付けます。

<#root>

```
ssl trust-point SELF-SIGNED
```

4. 証明書を確認します。

<#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. インターフェイスとの証明書の関連付けを確認します。

<#root>

#

show run all ssl

問題 2.ASDMまたはASA CLIを使用して証明書をインストールまたは更新する方法

ユーザは、ASDMまたはASA CLIを使用して証明書をインストールまたは更新する手順を明確にすることを望んでいます。

推奨される対処法

証明書のインストールと更新については、次のガイドを参照してください。

- ASA:SSL Digital Certificate Installation and Renewal（SSLデジタル証明書のインストールと更新）
- CLIで管理されるASAでの証明書のインストールと更新

ASDMの脆弱性に関する問題

このセクションでは、ASDMの脆弱性に関連する最も一般的な問題について説明します。

問題 1.ASDMで検出された脆弱性

ASDM上で脆弱性を検出した場合。

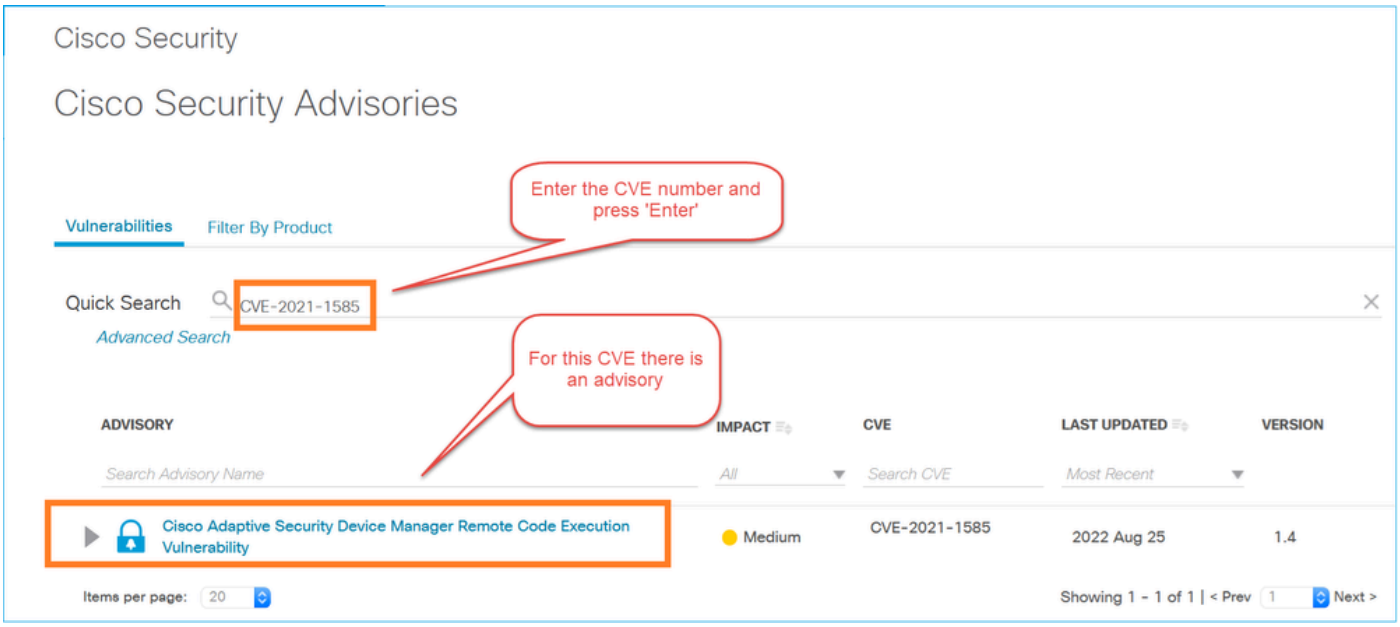
トラブルシューティング – 推奨手順

ステップ1:CVE IDを特定します(CVE-2023-21930など)。

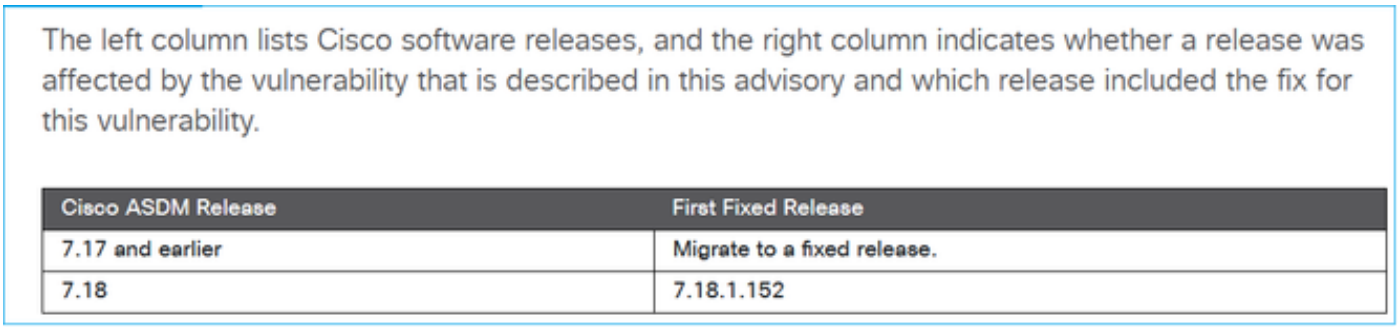
ステップ2：シスコセキュリティアドバイザリとCisco Bug SearchツールでCVEを検索します。

アドバイザリページに移動します。

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



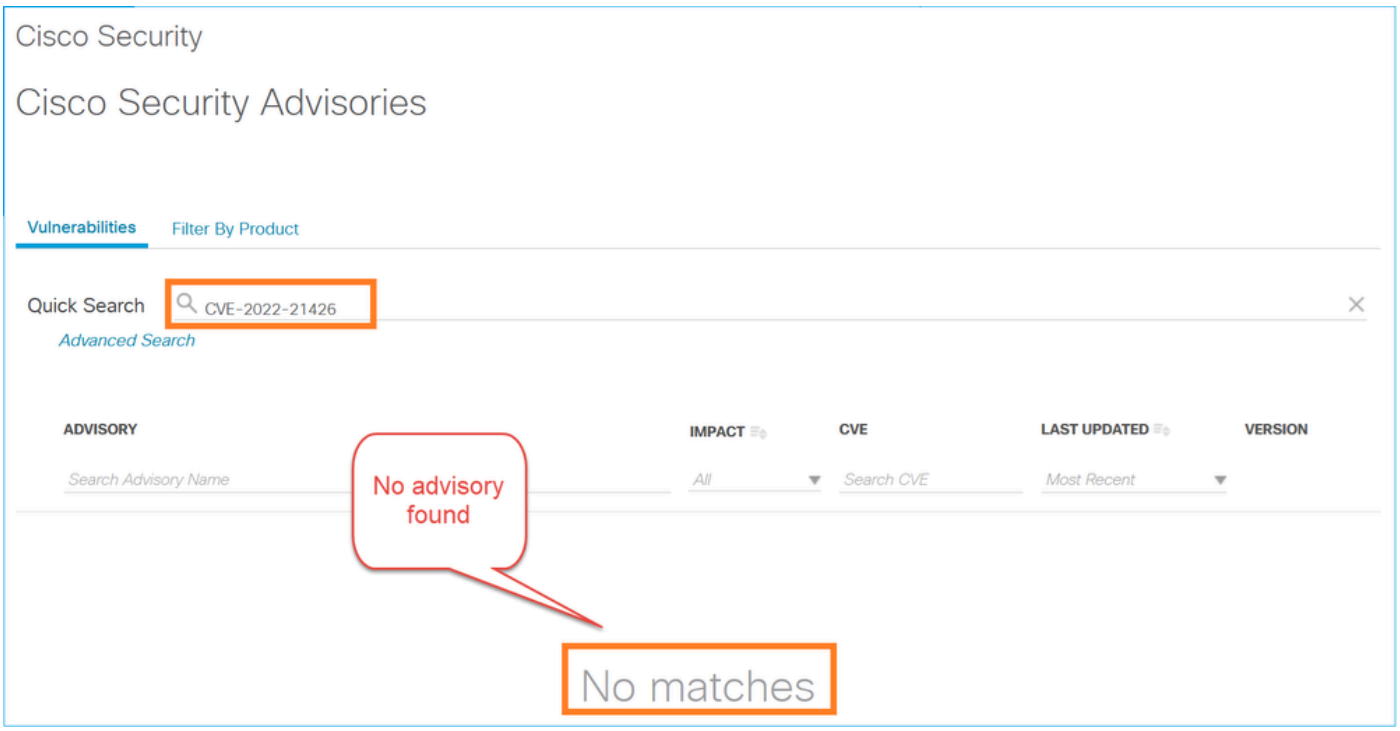
アドバイザリを開き、ASDMが影響を受けるかどうかを確認します。次に例を示します。

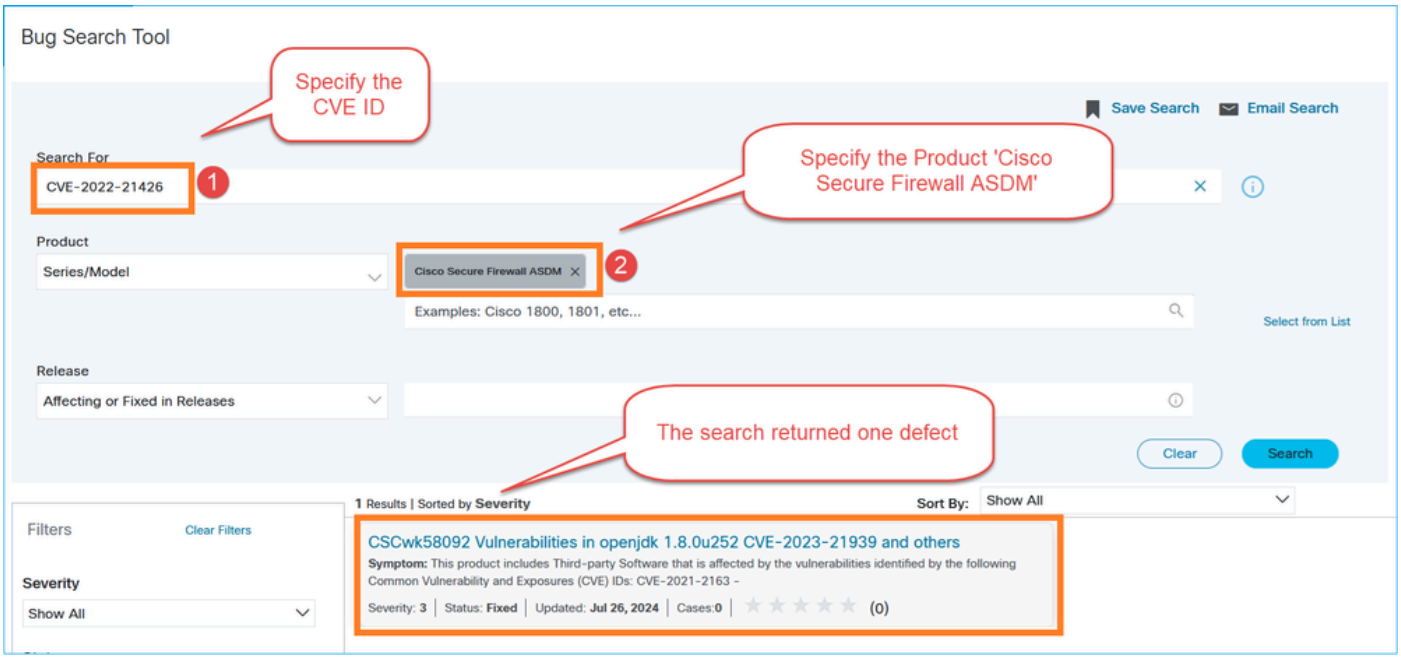


The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

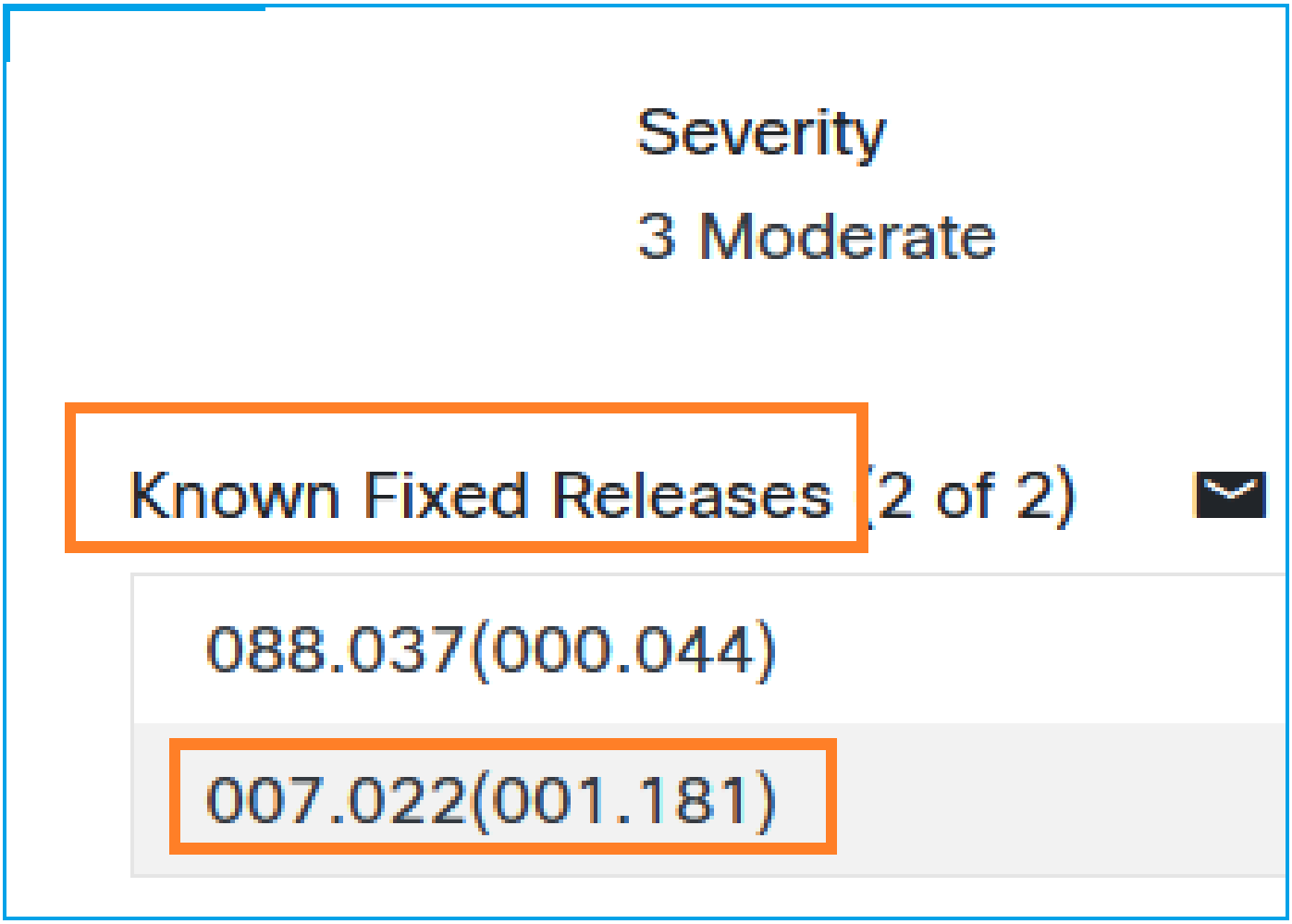
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

アドバイザリが見つからない場合は、Cisco Bug Search Tool(https://bst.cisco.com/bugsearch)





この場合、不具合が特定されています。これをクリックして詳細および「既知の修正済みリリース」セクションを確認します。



この不具合は、7.22.1.181 ASDMソフトウェアリリースで修正されています。

指定されたCVE IDに対するアドバイザリツールとバグ検索ツールでの検索で何も返されない場合

は、Cisco TACと協力して、ASDMがCVEの影響を受けるかどうかを確認する必要があります。

参考資料

- ASDM設定ガイド
- モデルごとのCisco ASAとASDMの互換性

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。