أستكشاف أخطاء الأمان والشهادة والضعف الخاصة ب ASDM TLS وإصلاحها

المحتويات

المقدمة

يصف هذا المستند عملية أستكشاف أخطاء ASDM وإصلاحها لأمان طبقة النقل (TLS) والشهادة ومشكلات الثغرات الأمنية.

الخلفية

يعد هذا المستند جزءا من سلسلة أستكشاف أخطاء مدير أجهزة Adaptive Security Appliance (ASDM) وإصلاحها مع هذه المستندات:

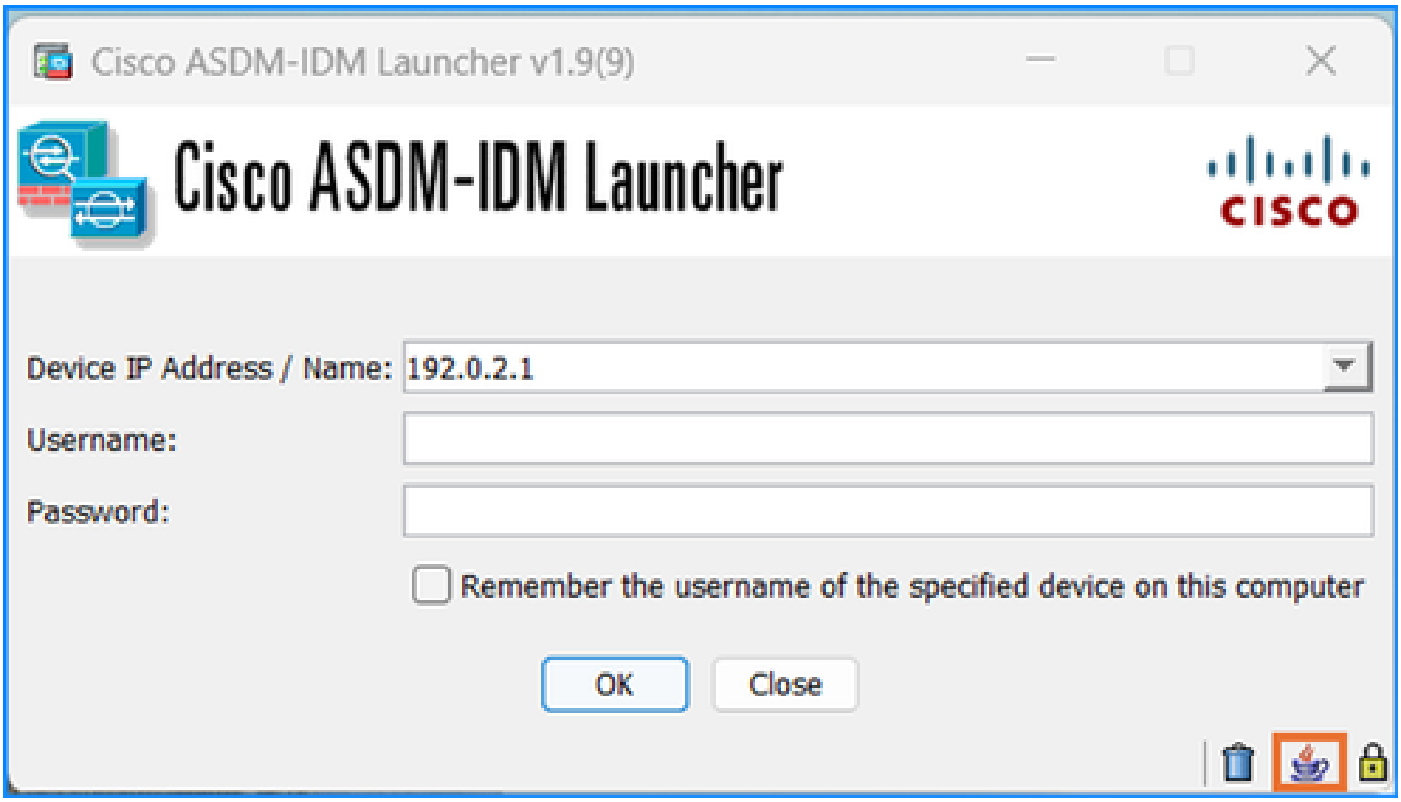
- [أستكشاف أخطاء تشغيل ASDM وإصلاحها](#)
- [أستكشاف أخطاء تكوين ASDM والمصادقة والمشاكل الأخرى وإصلاحها](#)
- [أستكشاف أخطاء ترخيص ASDM وترقيتها وتوافقها وإصلاحها](#)

مشاكل تشفير ASDM TLS

المشكلة 1. يتعذر على ASDM الاتصال بجدار الحماية بسبب مشاكل تشفير TLS

يتعذر على ASDM الاتصال بجدار الحماية. يلاحظ واحد أو أكثر من هذه الأعراض:

- يعرض ASDM رسائل الخطأ تعذر فتح الجهاز أو تعذر تشغيل إدارة الأجهزة من <ip>.
- يحتوي إخراج الأمر show ssl error على خطأ SSL lib. الوظيفة: ssl3_get_client_hello السبب: لا توجد رسالة تشفير مشتركة".
- تظهر سجلات وحدة تحكم Java الاستثناء javax.net.ssl.SSLHandshakeException: تم تلقي تنبيه قاتل: رسالة الخطأ 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)
```

أستكشاف الأخطاء وإصلاحها - الإجراءات الموصى بها

أحد الأسباب الرئيسية الشائعة للأعراض هو فشل مفاوضات مجموعة تشفير TLS بين ASDM و ASA. في هذه الحالات، على حسب تكوين التشفير، يحتاج المستخدم إلى ضبط الشهادة على جانب ASMD و/أو ASA.

انتقل عبر خطوة واحدة أو أكثر من هذه الخطوات حتى ينجح الاتصال:

1. في حالة إستخدام مجموعات تشفير TLS القوية مع OpenJRE، قم بتطبيق الحل البديل من البرنامج Cisco ق id CSCvv12542 "يجب أن يستخدم ASDM Open JRE شفرات أعلى بشكل افتراضي":
2. بدء تشغيل Notepad (التشغيل كمسؤول)
3. افتح الملف: C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security
4. البحث عن: crypto.policy=غير محدود
5. remove # أمام هذا السطر بحيث تتوفر جميع خيارات التشفير
6. حفظ

2. تغيير مجموعات تشفير TLS على 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
```

خيارات التشفير ل TLSv1.2:

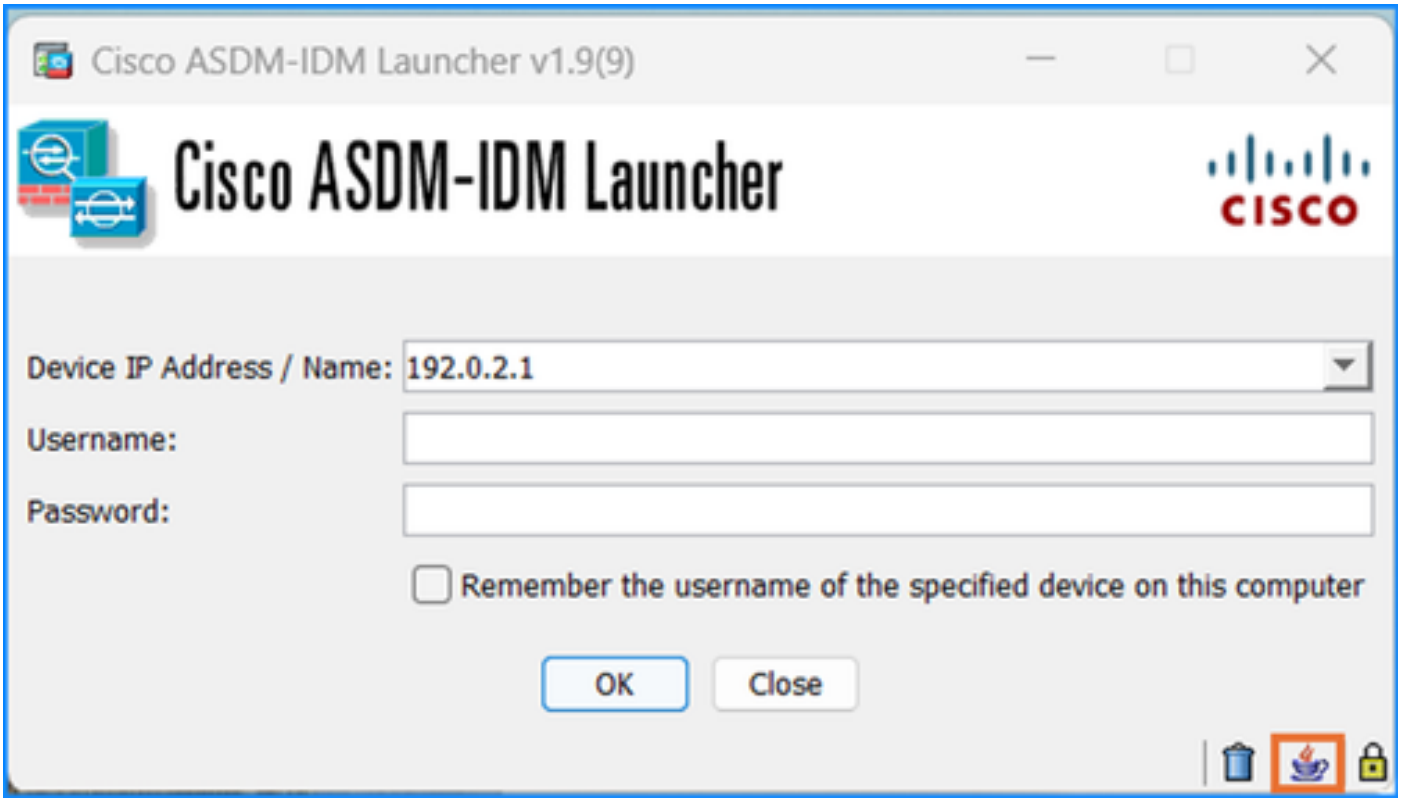
```
<#root>

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.
```

تحذير: يتم تطبيق التغييرات التي تحدث في أمر تشفير SSL على جدار الحماية بالكامل، بما في ذلك إتصالات VPN للوصول إلى الموقع أو الوصول عن بعد.

المشكلة 2. يتعذر على ASDM الاتصال بسبب فشل مصافحة TLS1.3

يتعذر على ASDM الاتصال بسبب فشل مصافحة TLS1.3.

تظهر سجلات وحدة تحكم Java Java.lang.IllegalArgumentException: رسالة خطأ TLSv1.3 وصة:



<#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)
```

أستكشاف الأخطاء وإصلاحها - الإجراءات الموصى بها

يجب دعم إصدار TLS 1.3 على كل من ASA و ASDM. TLS يدعم الإصدار 1.3 في ASA الإصدار 9.19.1 والإصدارات الأحدث (ملاحظات الإصدار الخاصة بسلسلة ASA لجدار الحماية الآمن من Cisco، 9.19(x)). يلزم توفر الإصدار 8u261 من Oracle Java أو إصدار أحدث لدعم TLS الإصدار 1.3 (ملاحظات الإصدار لـ Cisco Secure Firewall ASDM، 7.19(x)).

المراجع

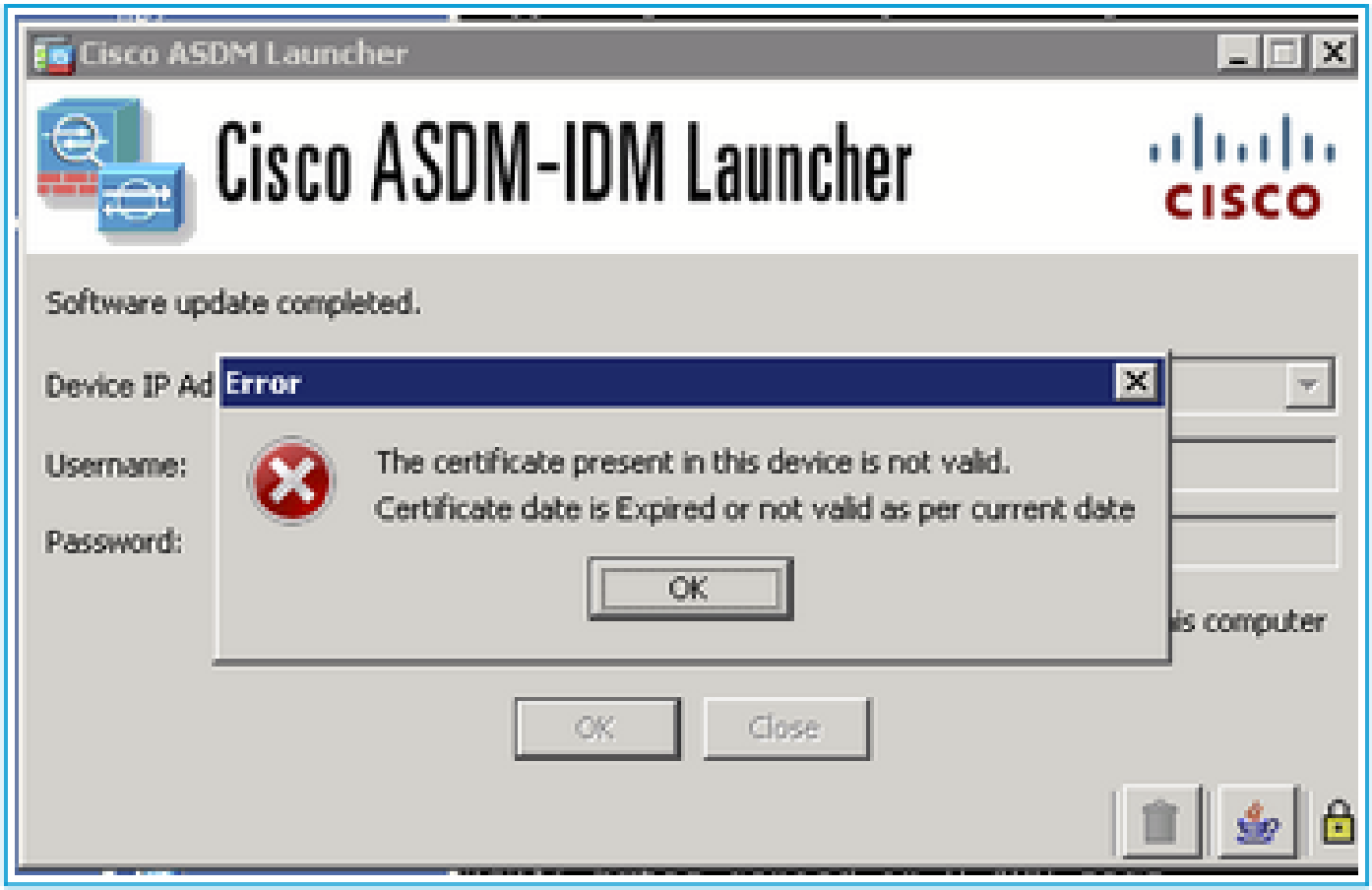
1. ملاحظات الإصدار الخاصة بسلسلة ASA لجدار الحماية الآمن من Cisco، 9.19(x)

2. ملاحظات الإصدار الخاصة ب Cisco Secure Firewall ASDM، 7.19(x)

مشاكل شهادات ASDM

المشكلة 1. الشهادة الموجودة في هذا الجهاز غير صالحة. تاريخ الشهادة منتهي الصلاحية أو غير صالح لكل تواريخ حالية. رسالة الخطأ

تظهر رسالة الخطأ عند تشغيل ASDM: "الشهادة الموجودة في هذا الجهاز غير صالحة. تاريخ الشهادة منتهي الصلاحية أو غير صالح لكل تواريخ حالية.



وثمة أعراض مماثلة موصوفة في ملاحظات الإصدار:

"الشهادة الموقعة ذاتيا الخاصة ب ASDM غير صالحة بسبب عدم تطابق الوقت والتاريخ مع ASA — توقف ASDM بالتحقق من صحة شهادة SSL الموقعة ذاتيا، وإذا لم يكن تاريخ ASA ضمن تاريخ إصدار الشهادة وانتهاء صلاحيتها، فلن يتم تشغيل ASDM. راجع ملاحظات توافق ASDM

استكشاف الأخطاء وإصلاحها - الإجراءات الموصى بها

1. التحقق من الشهادات منتهية الصلاحية وتأكيدها:

<#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. في واجهة سطر الأوامر (CLI) الخاصة ب ASA، قم بإزالة السطر ssl trust-point <cert> <interface>، حيث يكون <interface> هو الاسم المستخدم لاتصالات ASDM. يستخدم ASA شهادة موقعة ذاتيا لاتصالات ASDM.
2. في حالة عدم وجود شهادة موقعة ذاتيا، قم بإنشاء واحدة. في هذا المثال، يتم إستخدام اسم التوقيع الذاتي كاسم نقطة حقيقي:

<#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. إقران الشهادة التي تم إنشاؤها بالواجهة:

```
<#root>

ssl trust-point SELF-SIGNED
```

4. التحقق من الشهادة:

```
<#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. تحقق من اقتران الشهادة بالواجهة:

```
<#root>

#

 show run all ssl
```

المشكلة 2. كيف يمكن تثبيت الشهادات أو تجديدها باستخدام واجهة سطر الأوامر (CLI) ل ASDM أو ASA؟

يريد المستخدمون توضيح خطوات تثبيت الشهادات أو تجديدها باستخدام واجهة سطر الأوامر (CLI) ل ASDM أو ASA.

الإجراءات الموصى بها

ارجع إلى الأدلة لتثبيت الشهادات وتجديدها:

- ASA: تثبيت شهادة SSL الرقمية وتجديدها
- تثبيت وتجديد الشهادات على ASA المدارة بواسطة CLI (واجهة سطر الأوامر)

مشاكل الثغرات في إدارة قاعدة بيانات المحول (ASDM)

يغطي هذا القسم المشاكل المتعلقة بنقاط الضعف في إدارة قاعدة بيانات المحول (ASDM) الأكثر شيوعا.

المشكلة 1. الضعف المكتشف في ASDM

في حالة اكتشاف قابلية للتأثر على ASDM.

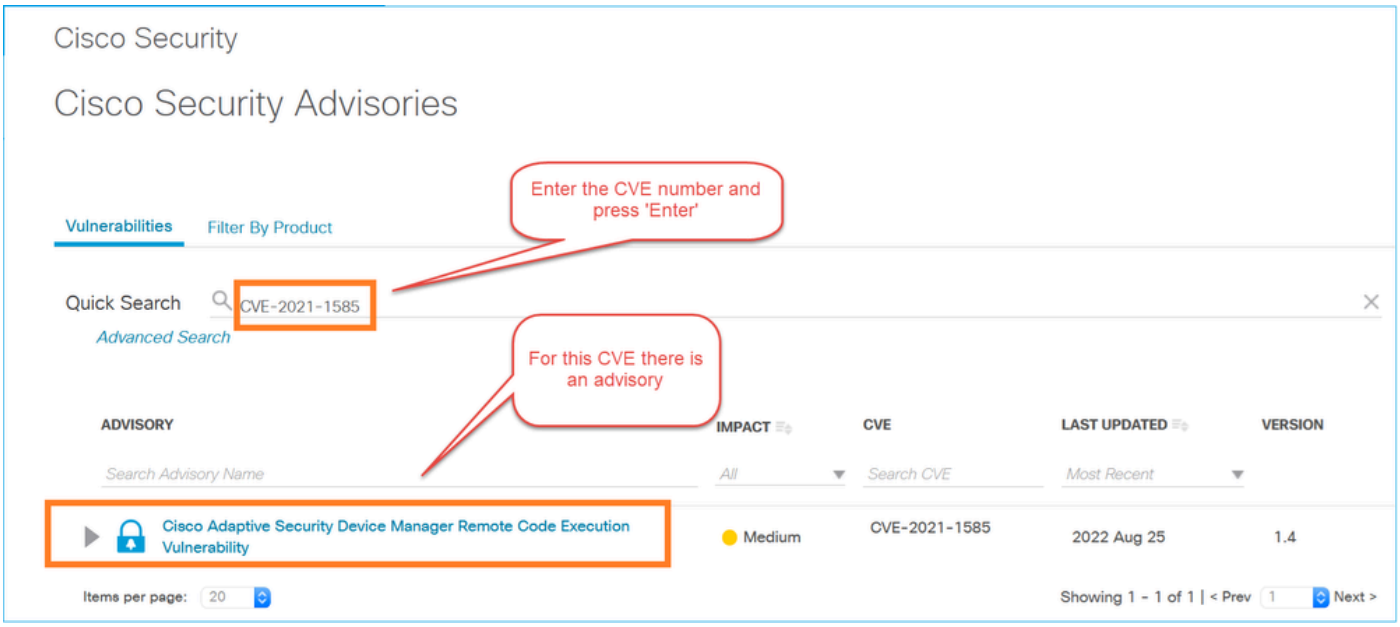
أستكشاف الأخطاء وإصلاحها - الخطوات الموصى بها

الخطوة 1: تعريف معرف CVE (على سبيل المثال، CVE-2023-21930)

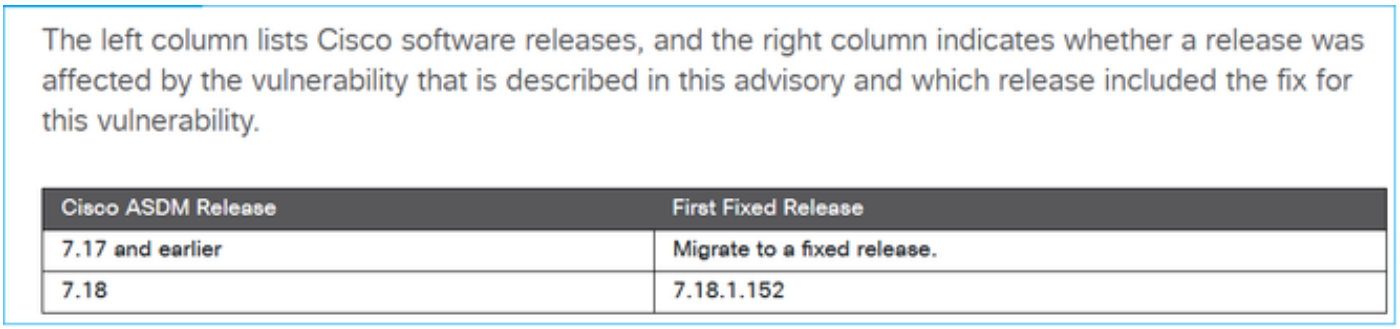
الخطوة 2: ابحث عن CVE في إرشادات الأمان من Cisco وأداة البحث عن الأخطاء من Cisco:

انتقل إلى الصفحة الاستشارية:

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



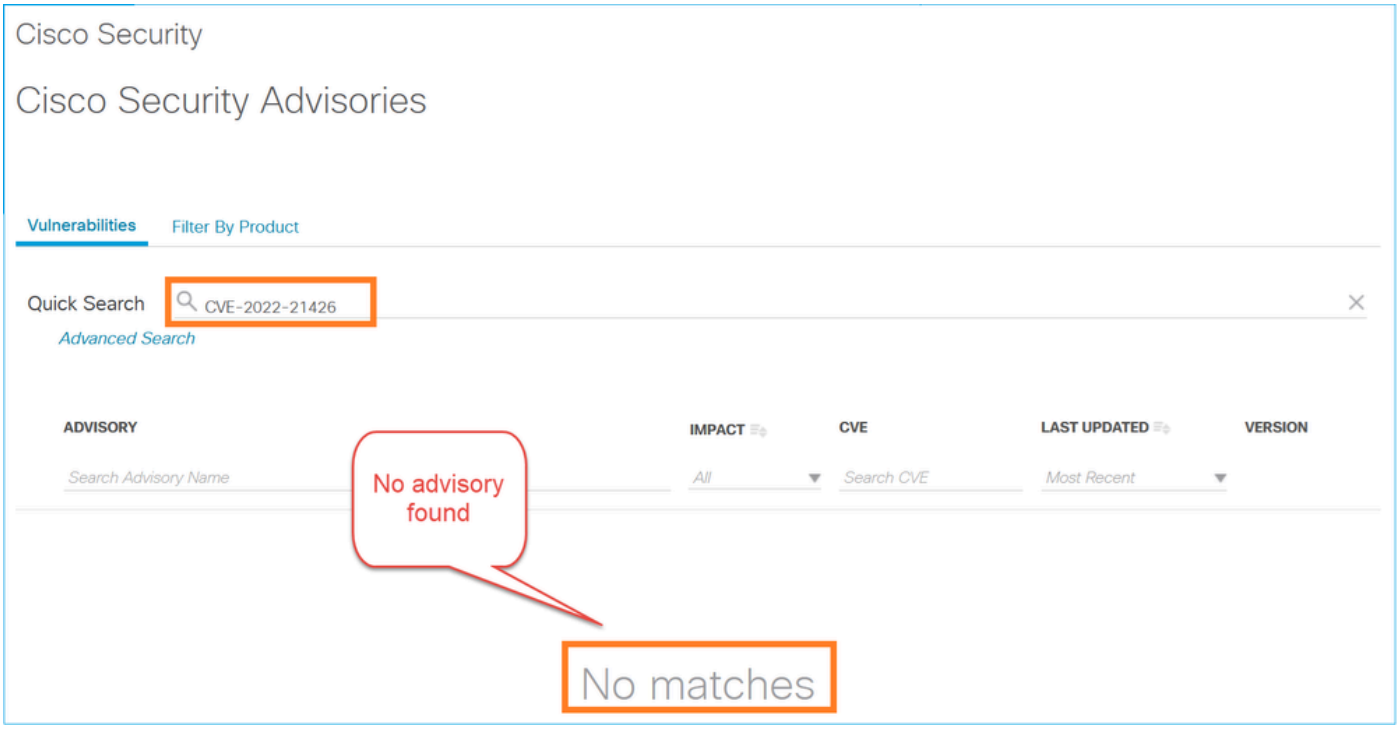
افتح الاستشارة وتحقق مما إذا كان ASDM يتأثر، على سبيل المثال:

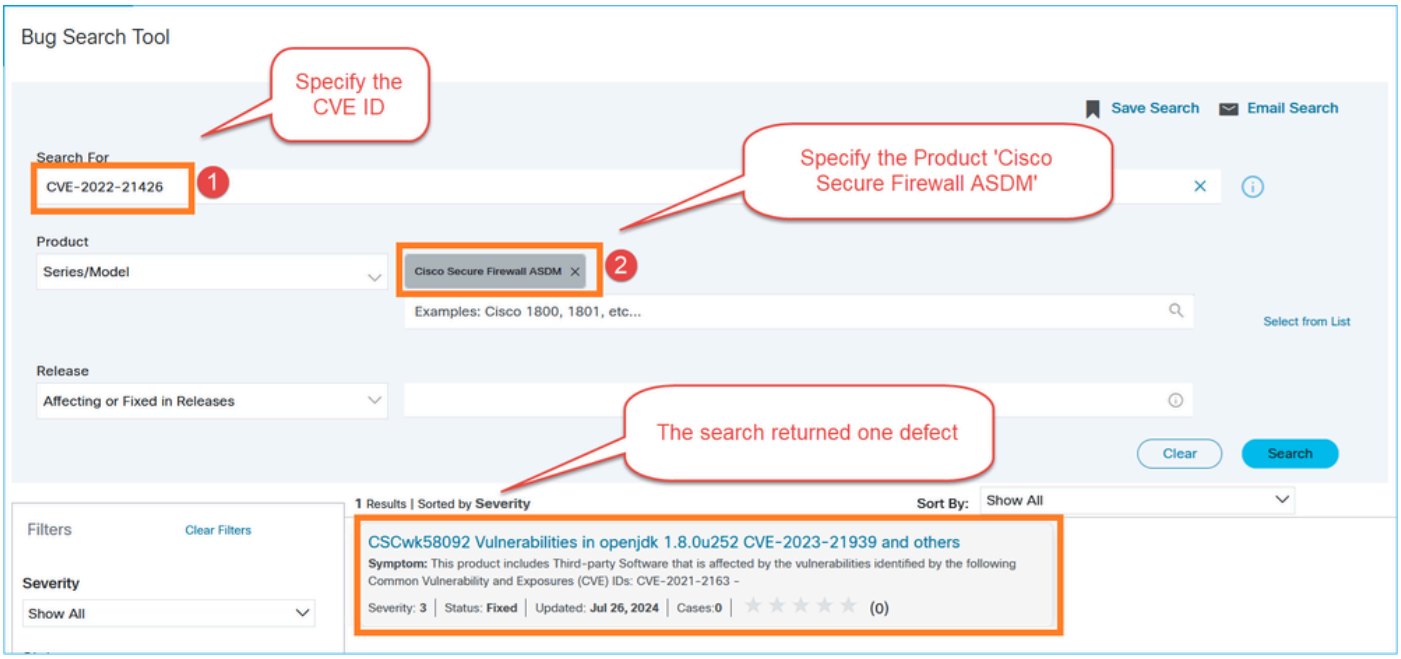


The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

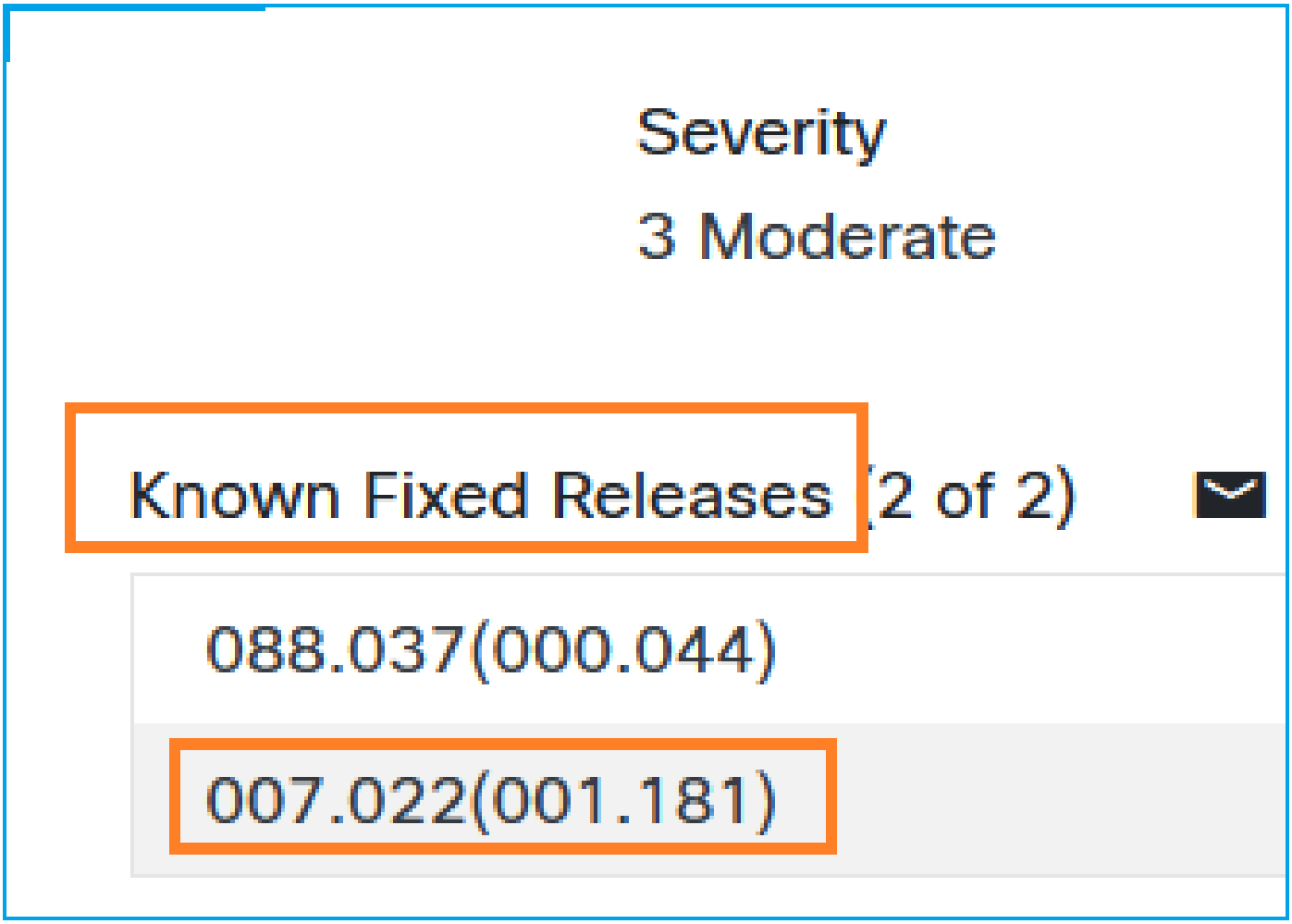
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

في حالة عدم العثور على نصيحة، ابحث عن معرف CVE في أداة البحث عن الأخطاء من Cisco (https://bst.cisco.com/bugsearch)





وفي هذه الحالة جرى تحديد خلل. انقر فوق هذا الخيار وتحقق من تفاصيله ومن قسم "الإصدارات المعروفة التي تم إصلاحها":



تم إصلاح الخلل في إصدار برنامج ASDM 7.22.1.181.

إذا لم ترجع عمليات البحث في الأداة الاستشارية وأداة البحث عن الأخطاء الخاصة بمعرف CVE

المحدد أي شيء، فأنت بحاجة إلى العمل مع Cisco TAC لتوضيح ما إذا كان ASDM متأثرا ببروتوكول CVE.

المراجع

- أدلة تكوين ASDM
- توافق Cisco ASA و ASDM لكل نموذج

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).