排除ASDM TLS安全、證書和漏洞問題

目錄

簡介

本文檔介紹ASDM傳輸層安全(TLS)安全性、證書和漏洞問題的故障排除過程。

背景

本文檔是Adaptive Security Appliance Device Manager(ASDM)故障排除系列的一部分，本文檔包括以下文檔：

- 排除ASDM啟動問題
- 排除ASDM配置、身份驗證和其他問題
- 排除ASDM許可證、升級和相容性問題

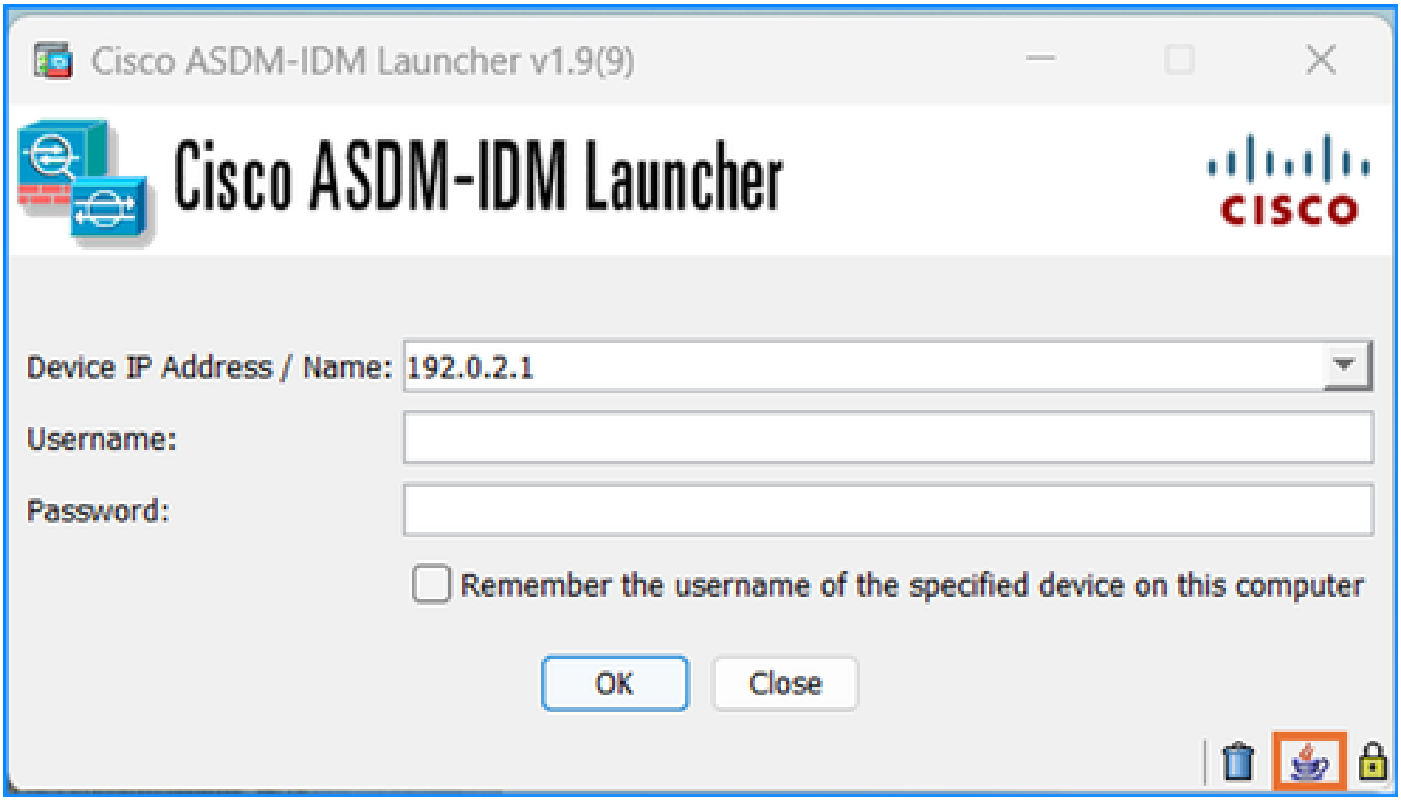
ASDM TLS密碼問題

問題1. 由於TLS密碼問題，ASDM無法連線到防火牆

ASDM無法連線到防火牆。觀察到以下一個或多個症狀：

- ASDM顯示「Couldn not open device」或「Unable to launch device manager from <ip>」錯誤消息。

- show ssl error命令的輸出包含「SSL lib error」。功能:ssl3_get_client_hello原因：無共用密碼」消息。
- Java控制檯日誌顯示「javax.net.ssl.SSLHandshakeException:收到致命警報：handshake_failure"錯誤消息：



<#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)
```

疑難排解 — 建議動作

這些症狀的常見根本原因是ASDM和ASA之間的TLS密碼套件協商失敗。在這些情況下，根據密碼配置，使用者需要調整ASMD和/或ASA端上的證書。

請執行以下一個或多個步驟直到連線成功：

1. 如果使用OpenJRE的ASDM，如果使用強式TLS密碼套件，請應用軟體錯誤ID CSCvv12542「ASDM open JRE預設應使用較高密碼」的變通方法：
2. 啟動記事本（以管理員身份運行）

3. 開啟檔案：C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security
4. 搜尋：crypto.policy=unlimited
5. 在該行前面刪除#，以便所有加密選項均可用
6. 儲存

2. 更改ASA上的TLS密碼套件。

<#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的密碼選項：

<#root>

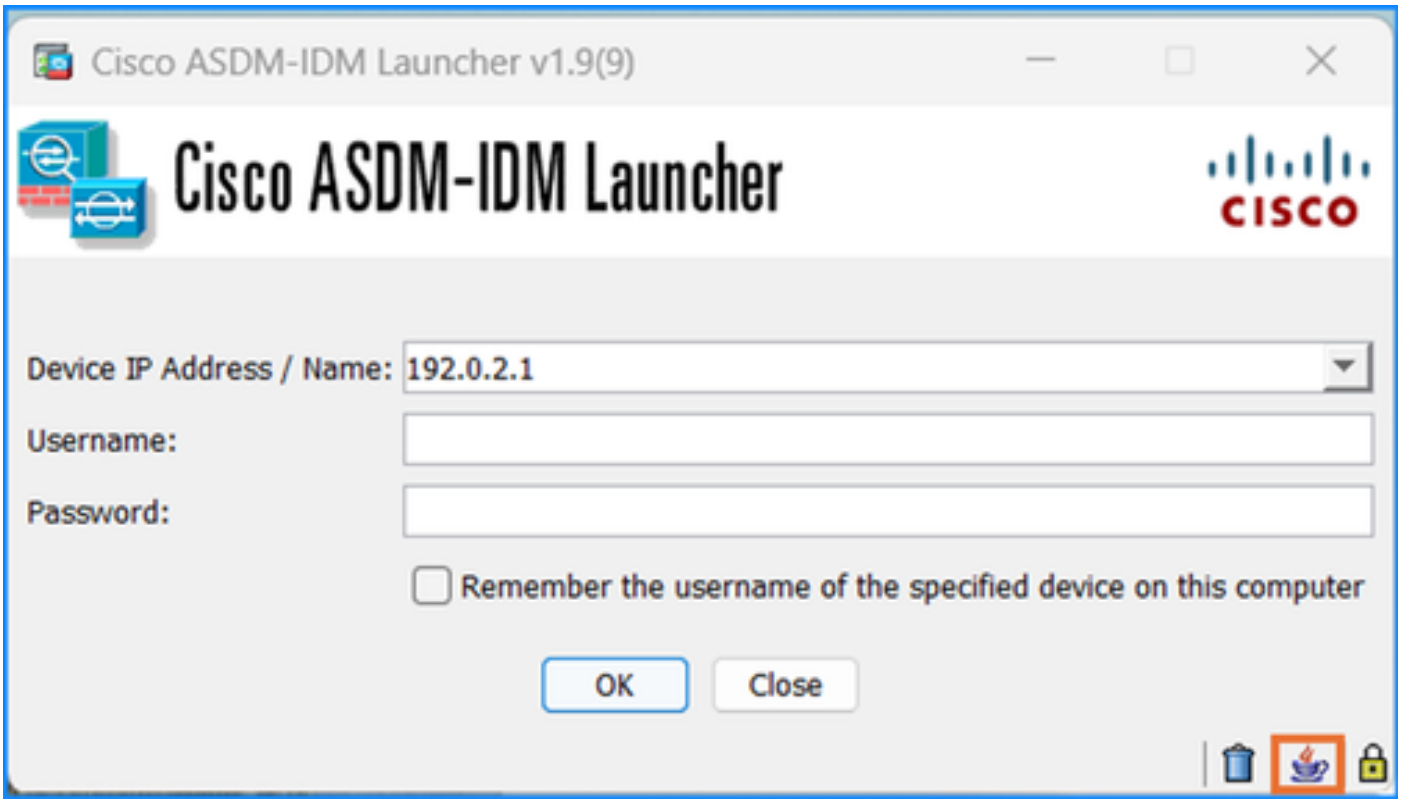
```
ASA(config)#
ssl cipher tlsv1.2 ?


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命令中的更改將應用到整個防火牆，包括站點到站點或遠端訪問VPN連線。

問題2. 由於TLS1.3握手失敗，ASDM無法連線到

由於TLS1.3握手失敗，ASDM無法連線到。

Java控制檯日誌顯示"java.lang.IllegalArgumentException:TLSv1.3"錯誤消息：



<#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)
```

疑難排解 — 建議動作

ASA和ASDM都必須支援TLS 1.3版本。 ASA 9.19.1及更高版本支援TLS 1.3版(Cisco Secure Firewall ASA系列9.19(x)發行說明)。 需要Oracle Java版本8u261或更高版本才能支援TLS版本1.3(Release Notes for Cisco Secure Firewall ASDM ， 7.19(x))。

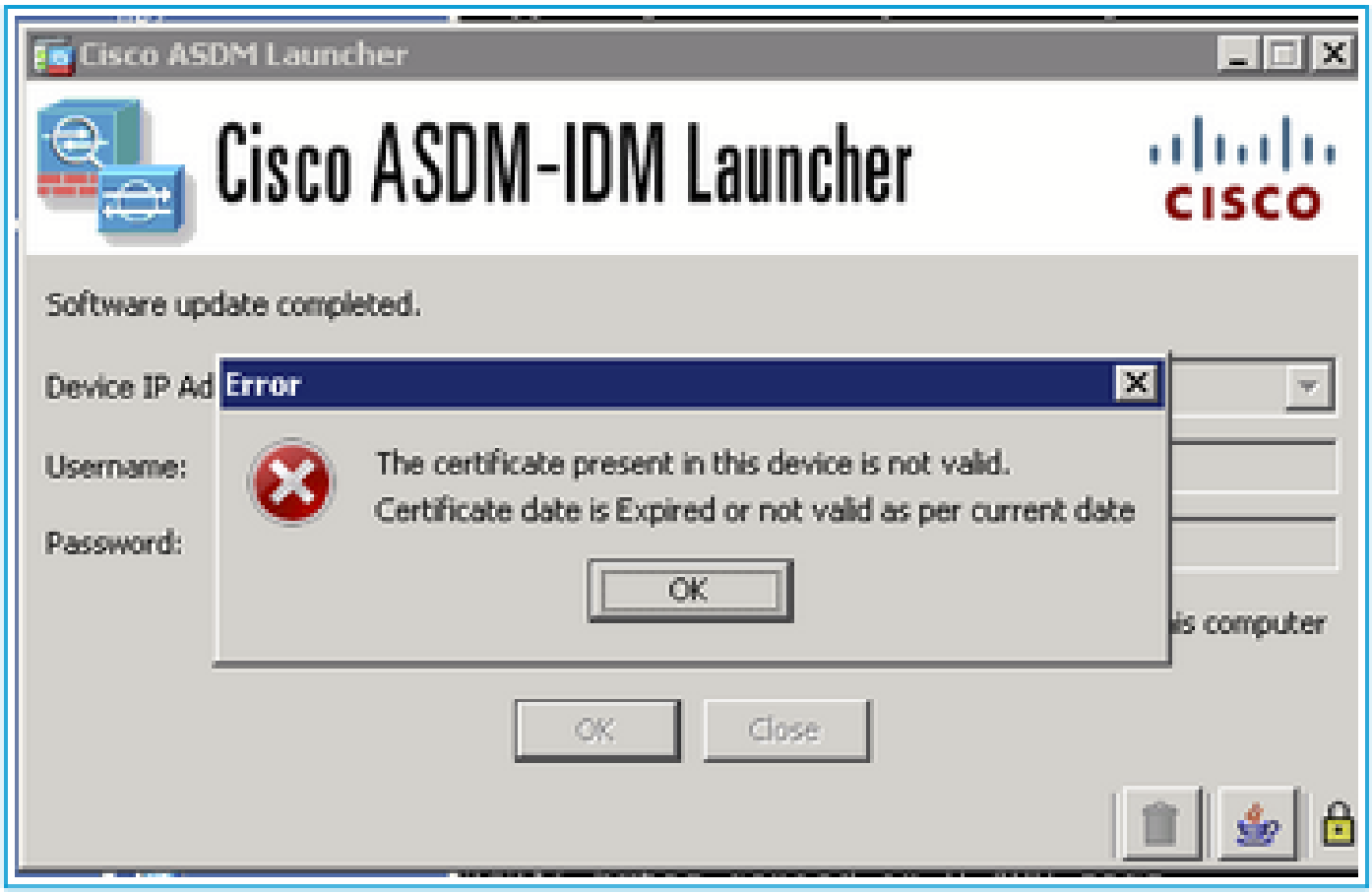
參考資料

1. 思科安全防火牆ASA系列9.19(x)版本說明
2. 思科安全防火牆ASDM 7.19(x)版本說明

ASDM證書問題

問題1.「此裝置中的證書無效。根據當前日期，證書日期已過期或無效。" 錯誤消息

運行ASDM時會顯示錯誤消息：「此裝置中的證書無效。根據當前日期，證書日期已過期或無效。"



版本說明中介紹了類似症狀：

「由於與ASA的時間和日期不匹配，ASDM的自簽名證書無效 — ASDM驗證自簽名SSL證書，如果ASA的日期不在證書的Issued On和Expires On date內，則ASDM將不會啟動。參見 ASDM相容性說明

疑難排解 — 建議動作

1. 檢查並確認過期的證書：

<#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. 在ASA命令列介面(CLI)中，刪除ssl trust-point <cert> <interface>行，其中<interface> 是用於ASDM連線的名稱。ASA對ASDM連線使用自簽名證書。
2. 如果沒有自簽名證書，請生成一個。在本示例中，SELF-SIGNED名稱用作真點名稱：

```
<#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. 將生成的證書與介面關聯：

<#root>

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

4.驗證憑證：

<#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.驗證與介面的憑證關聯：

```
<#root>

#

 show run all ssl
```

問題2.如何使用ASDM或ASA CLI安裝或續訂證書？

使用者希望澄清使用ASDM或ASA CLI安裝或續訂證書的步驟。

建議的操作

請參閱指南以安裝和續訂證書：

- ASA:安裝和更新 SSL 數位憑證

- [在CLI管理的ASA上安裝並續訂證書]

ASDM漏洞問題

本節介紹最常見的ASDM漏洞相關問題。

問題1.在ASDM上檢測到的漏洞

以防您在ASDM上檢測到漏洞。

疑難排解 — 建議步驟

步驟 1:標識CVE ID(例如，CVE-2023-21930)

步驟 2:在思科資安顧問和思科錯誤搜尋工具中搜尋CVE:

導航至建議頁面：

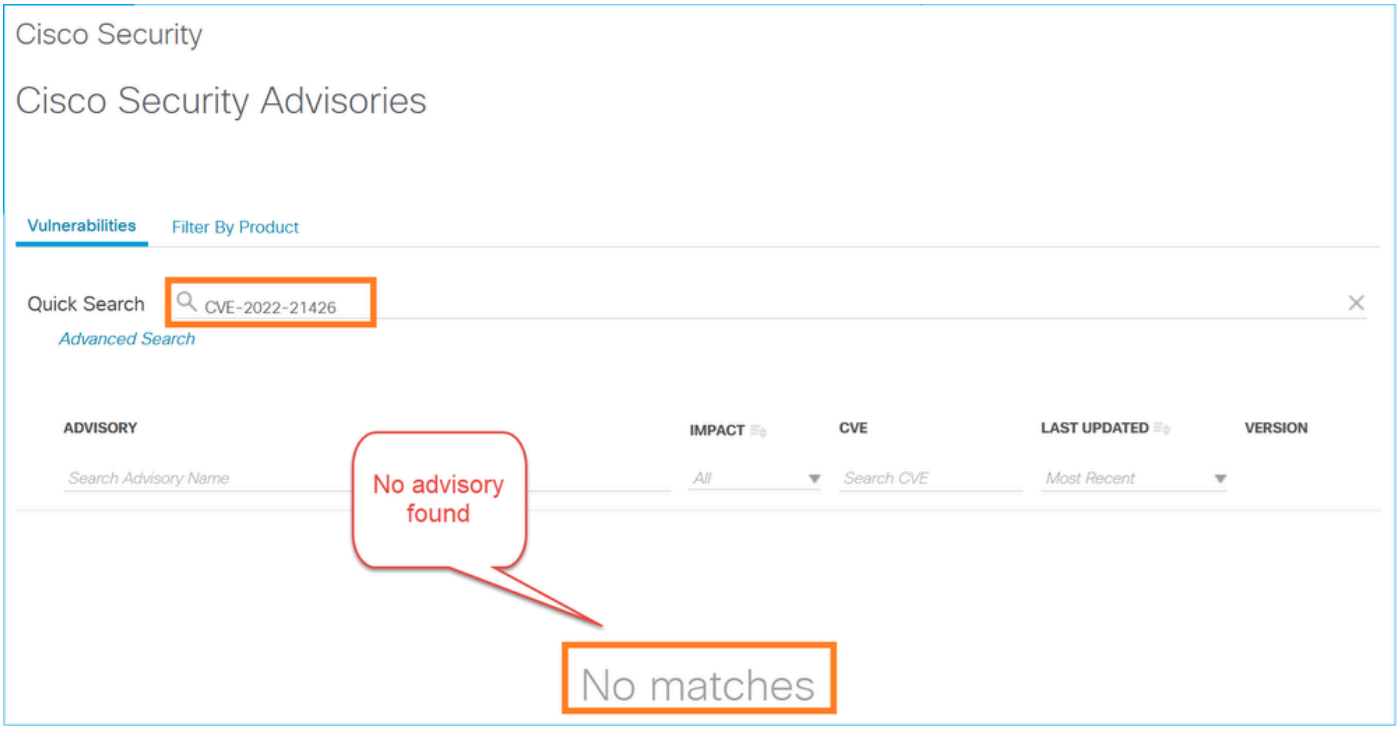
https://sec.cloudapps.cisco.com/security/center/publicationListing.x

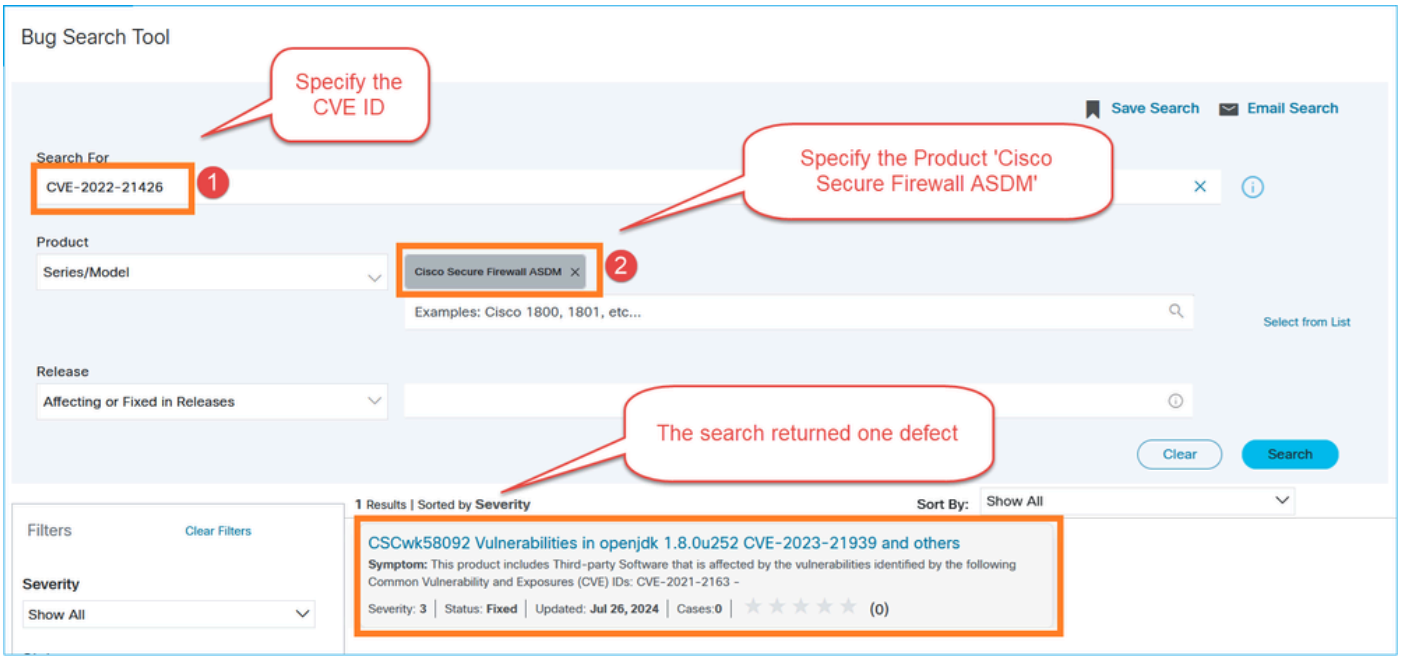
開啟建議並檢查ASDM是否受到影響，例如：

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.

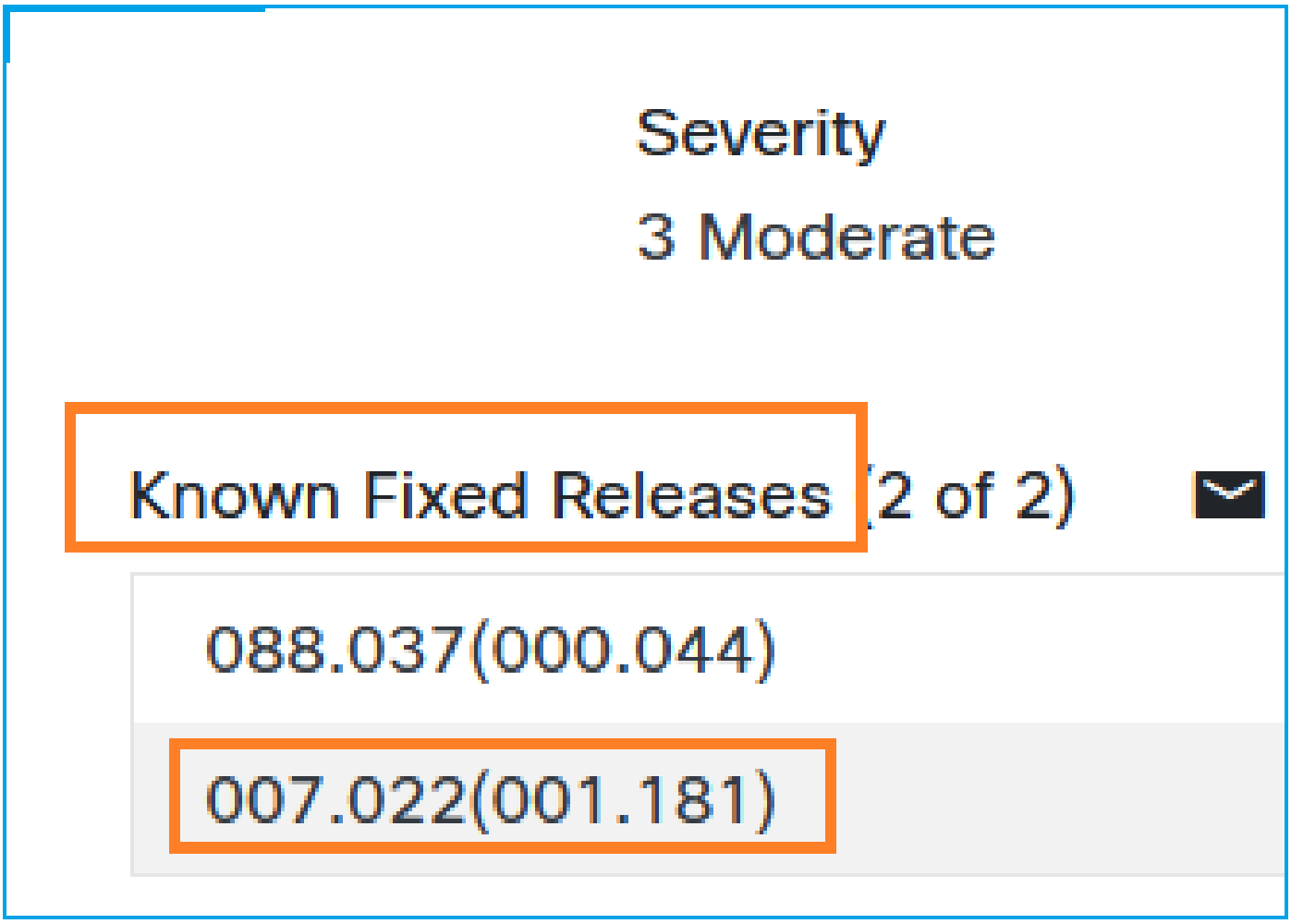
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

如果沒有找到建議，請在思科錯誤搜尋工具中搜尋CVE ID(https://bst.cisco.com/bugsearch)





在此案例中識別出缺陷。按一下它並檢查其詳細資訊和「已知修正版本」部分：



該缺陷已在7.22.1.181 ASDM軟體版本中修復。

如果顧問工具和錯誤搜尋工具中對指定CVE ID的搜尋沒有傳回任何內容，則需要與思科TAC合作，以澄清ASDM是否受CVE影響。

參考資料

- ASDM配置指南
- 每種型號的Cisco ASA和ASDM相容性

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。