排除ASDM TLS安全、证书和漏洞问题

目录

简介

本文档介绍ASDM传输层安全(TLS)安全、证书和漏洞问题的故障排除过程。

背景

本文档是自适应安全设备管理器(ASDM)故障排除系列的一部分，包括以下文档：

- 排除ASDM启动问题
- 排除ASDM配置、身份验证和其他问题
- 排除ASDM许可证、升级和兼容性问题

ASDM TLS密码问题

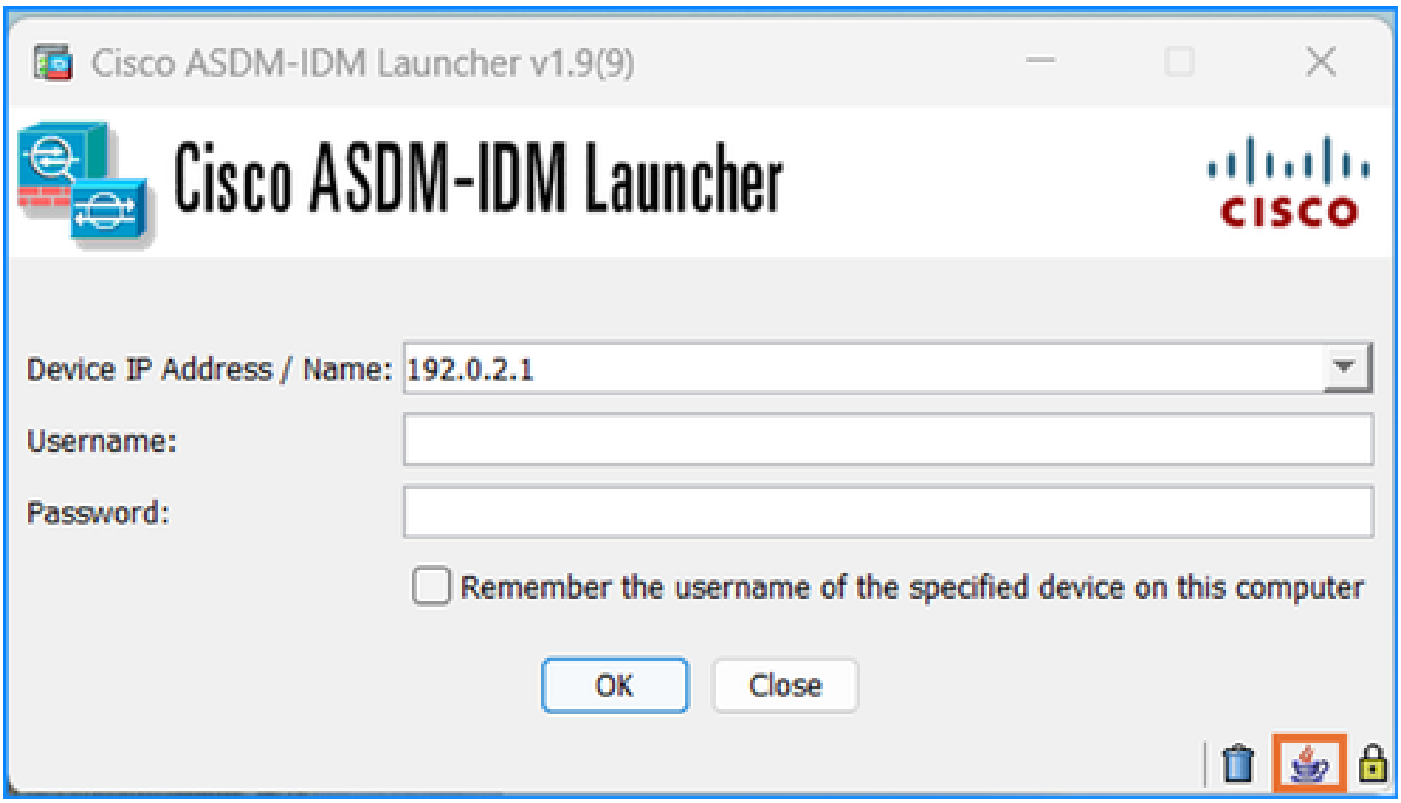
问题 1. 由于TLS密码问题，ASDM无法连接到防火墙

ASDM无法连接到防火墙。观察到以下一个或多个症状：

- ASDM显示“Could not open device”或“Unable to launch device manager from <ip>”错误消息。
- show ssl error命令的输出包含“SSL lib error。功能:ssl3_get_client_hello原因：no shared

cipher”消息。

- Java控制台日志显示“javax.net.ssl.SSLHandshakeException:收到致命警报：handshake_failure"错误消息：



<#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)
```

故障排除 — 建议的操作

这些症状的常见根本原因是ASDM和ASA之间的TLS密码套件协商失败。在这些情况下，根据密码配置，用户需要调整ASMD和/或ASA端的证书。

请执行以下一个或多个步骤直至连接成功：

1. 对于使用OpenJRE的ASDM，如果使用强TLS密码套件，请应用软件Cisco bug ID CSCvv12542“ASDM open JRE默认情况下应使用更高的密码”的解决方法：
2. 启动记事本（以管理员身份运行）
3. 打开文件：C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security

4. 搜索：crypto.policy=unlimited
5. 在该行前面删除#，以便所有加密选项都可用
6. 保存

2. 更改ASA上的TLS密码套件。

<#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的密码选项：

<#root>

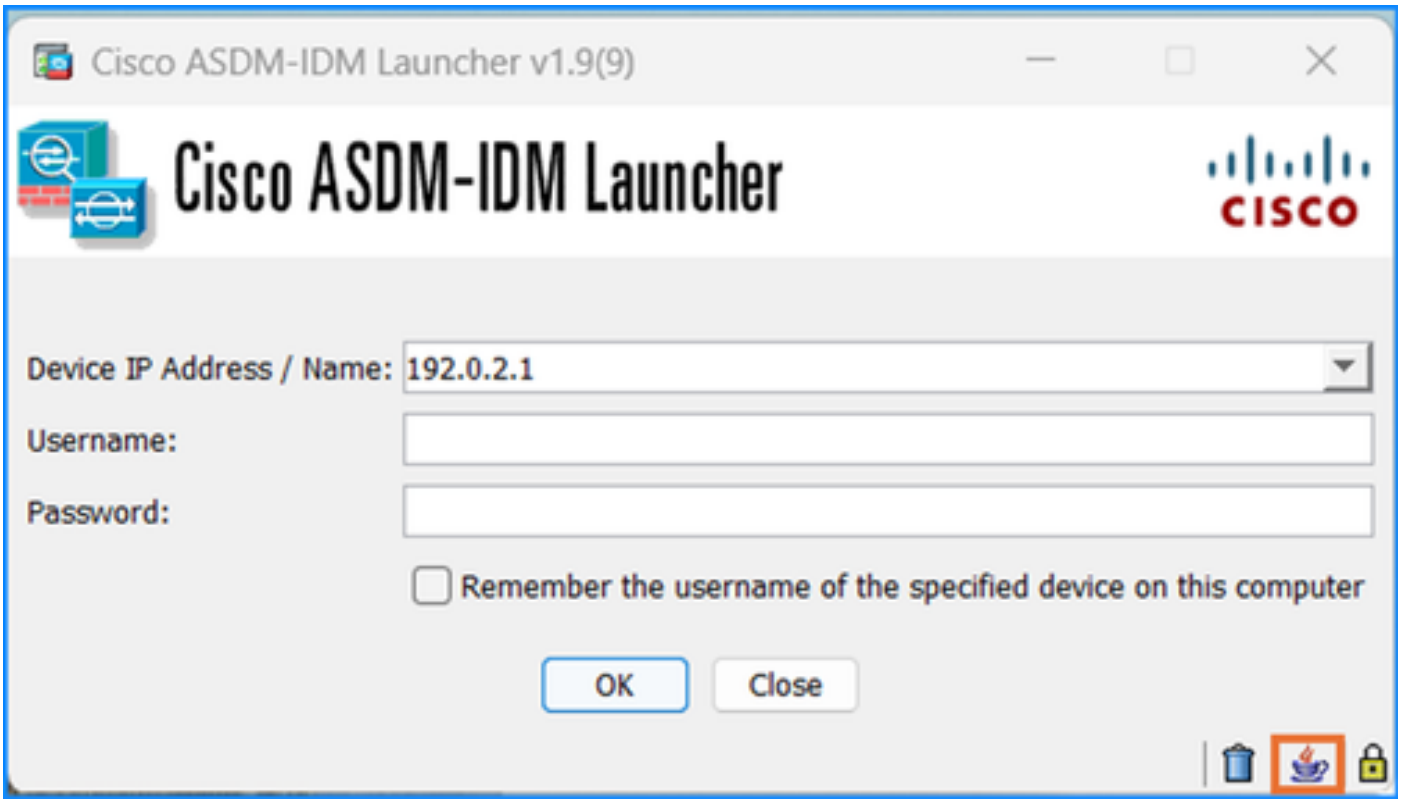
```
ASA(config)#

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命令中的更改应用于整个防火墙，包括站点到站点或远程访问VPN连接。

问题 2. 由于TLS1.3握手失败，ASDM无法连接到

由于TLS1.3握手失败，ASDM无法连接到。

Java控制台日志显示“java.lang.IllegalArgumentException:TLSv1.3”错误消息：



<#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)
```

故障排除 — 建议的操作

ASA和ASDM都必须支持TLS 1.3版本。 ASA版本9.19.1及更高版本支持TLS 1.3版(Cisco Secure Firewall ASA系列9.19(x)版本说明)。 需要Oracle Java版本8u261或更高版本才能支持TLS版本1.3(Cisco Secure Firewall ASDM 7.19(x)发行版本注释)。

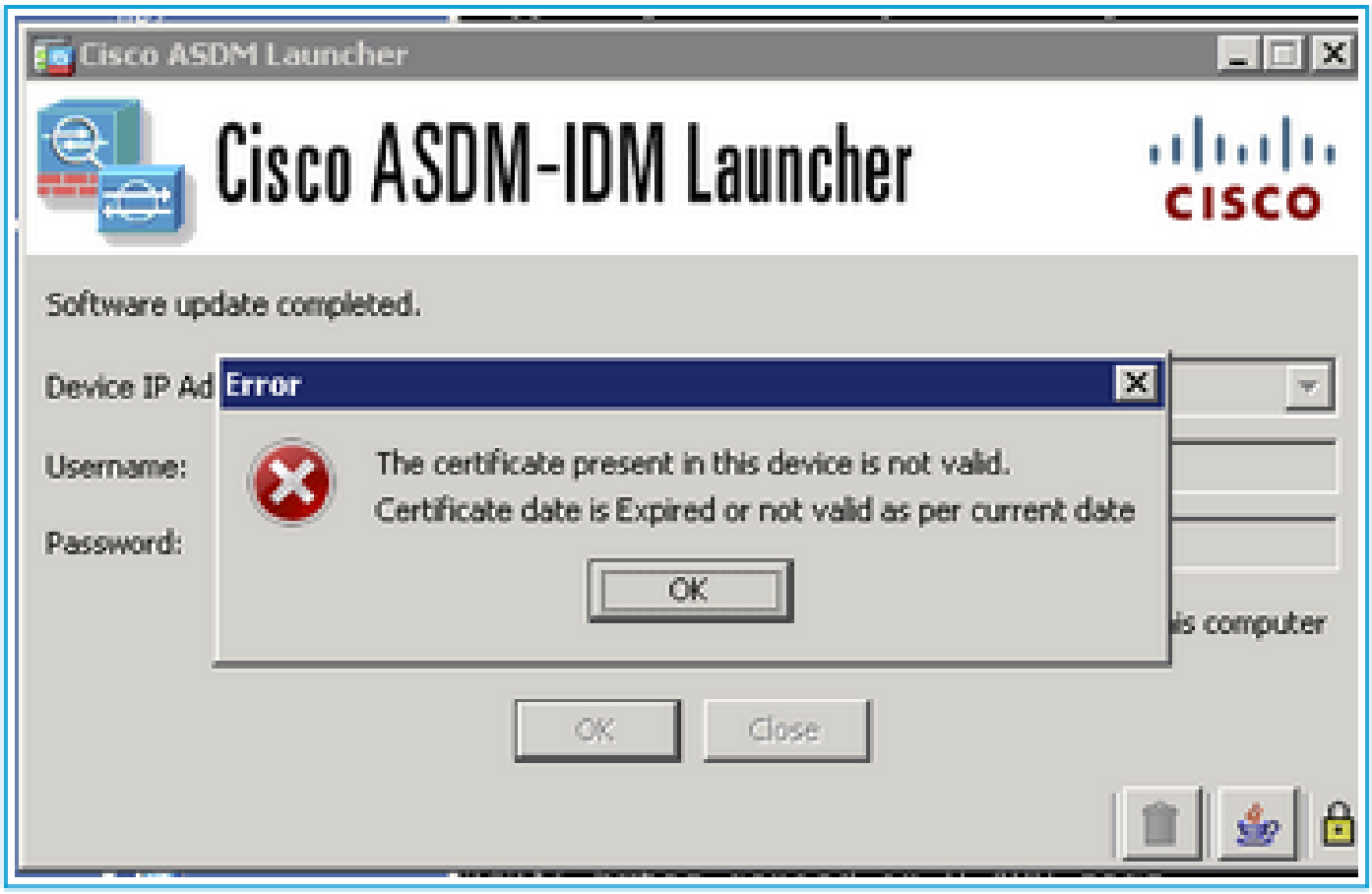
参考

1. 思科安全防火墙ASA系列9.19(x)版本说明
2. 思科安全防火墙ASDM 7.19(x)版本说明

ASDM证书问题

问题1. “此设备中的证书无效。根据当前日期，证书日期已过期或无效。" 错误消息

运行ASDM时会显示错误消息：“此设备中的证书无效。根据当前日期，证书日期已过期或无效。"



版本说明中介绍了类似的症状:

“由于与ASA的时间和日期不匹配，ASDM的自签名证书无效 — ASDM验证自签名SSL证书，如果ASA的日期不在证书的Issued On和Expires On日期内，ASDM将不会启动。参见 ASDM兼容性说明

故障排除 — 建议的操作

1. 检查并确认过期的证书：

```
<#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命令行界面(CLI)中，删除ssl trust-point <cert> <interface>行，其中<interface> 是用于ASDM连接的名称。ASA对ASDM连接使用自签名证书。
2. 如果没有自签名证书，请生成一个证书。在本示例中，SELF-SIGNED名称用作真正的点名称：

```
<#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. 将生成的证书与接口关联：

<#root>

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

4.验证证书：

<#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.验证证书与接口的关联：

<#root>

#

```
 show run all ssl
```

问题2.如何使用ASDM或ASA CLI安装或更新证书？

用户希望使用ASDM或ASA CLI明确安装或更新证书的步骤。

推荐的操作

请参阅以下指南，安装并续订证书：

- ASA ：SSL 数字证书安装和续约
- 在CLI管理的ASA上安装和更新证书

ASDM漏洞问题

本节介绍最常见的ASDM漏洞相关问题。

问题1.在ASDM上检测到的漏洞

以防您在ASDM上检测到漏洞。

故障排除 — 建议的步骤

步骤 1：确定CVE ID(例如，CVE-2023-21930)

步骤 2：在Cisco Security Advisories和Cisco Bug Search工具中搜索CVE:

导航至咨询页面：

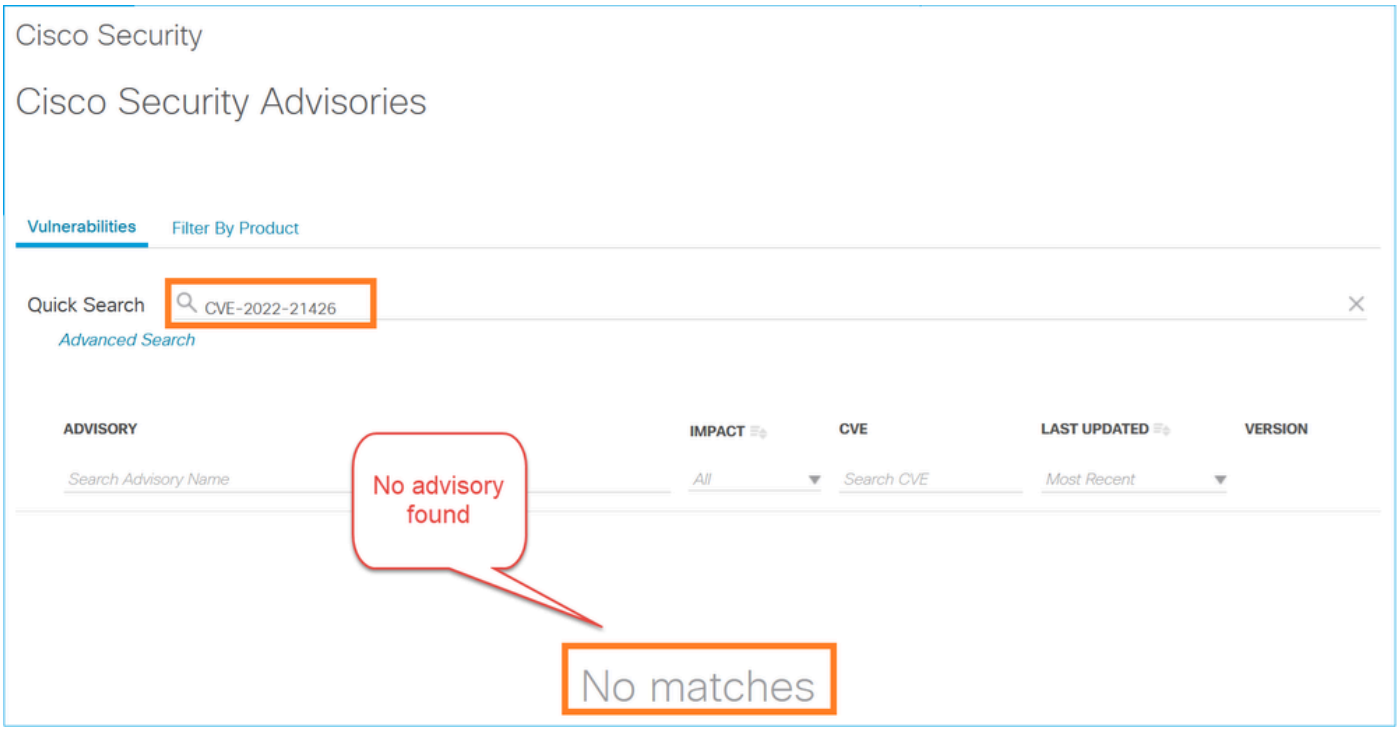
https://sec.cloudapps.cisco.com/security/center/publicationListing.x

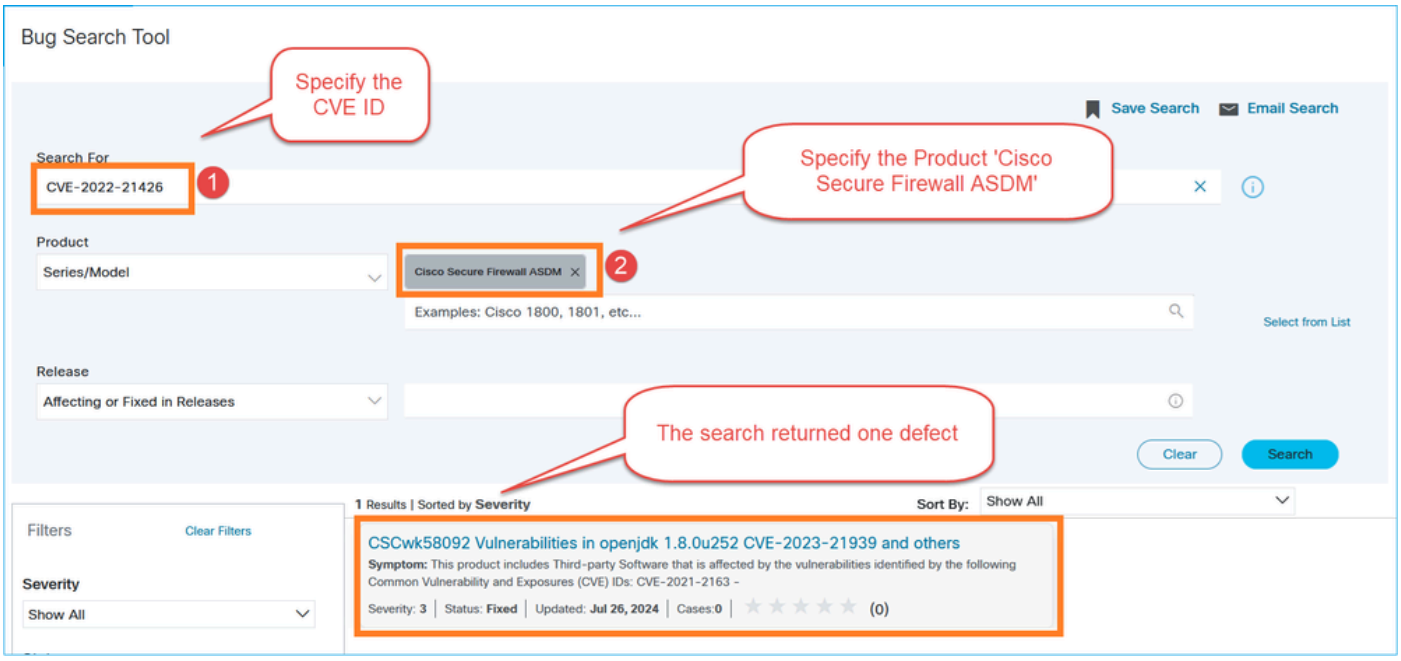
打开建议并检查ASDM是否受到影响，例如：

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.

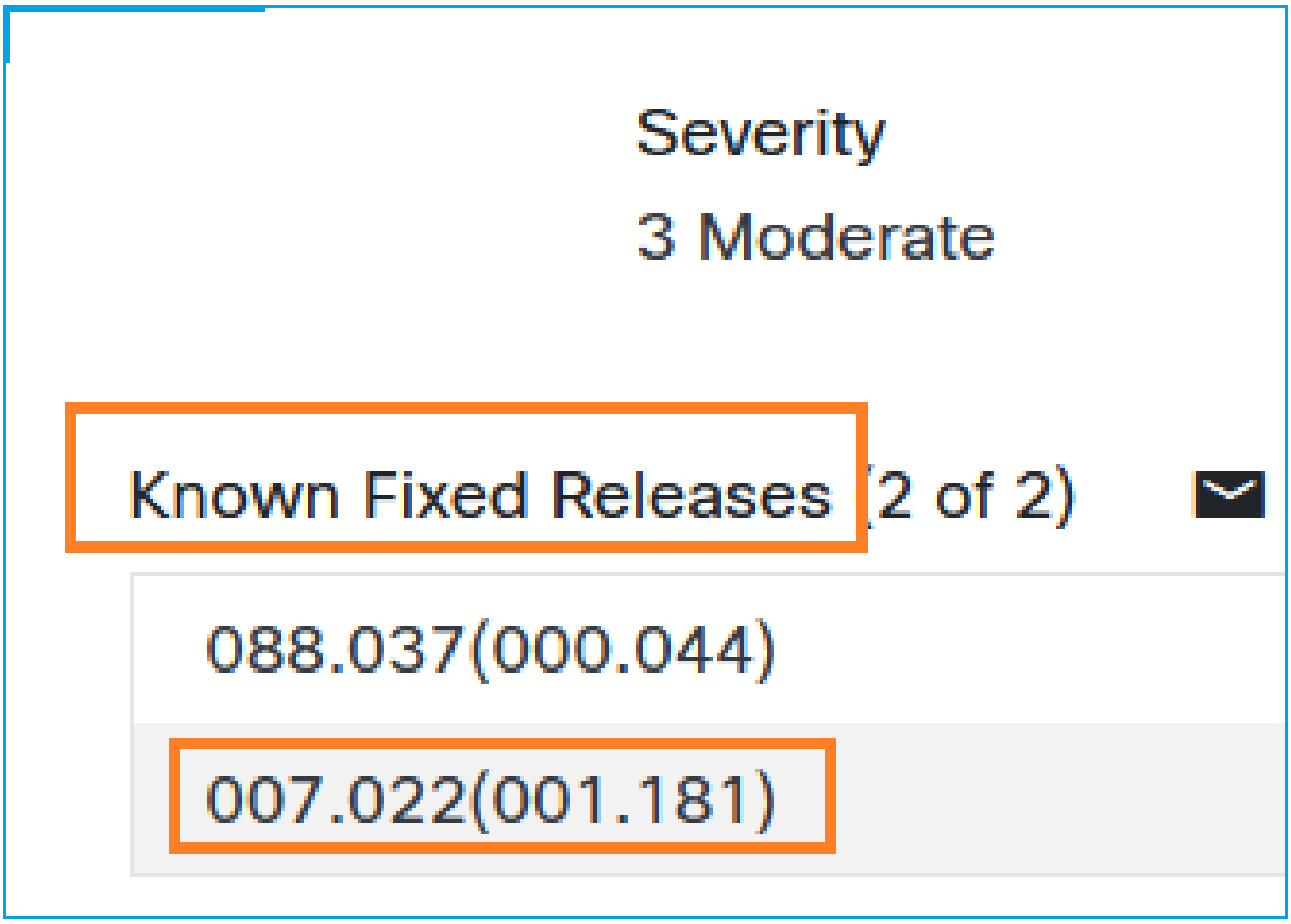
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

如果未找到建议，请在思科漏洞搜索工具(https://bst.cisco.com/bugsearch(E)





在本例中，识别出缺陷。点击并查看其详细信息和“已知固定版本”部分：



该缺陷在7.22.1.181 ASDM软件版本中得到修复。

如果顾问工具和漏洞搜索工具中对指定CVE ID的搜索未返回任何信息，您需要与思科TAC合作以澄清ASDM是否受到CVE的影响。

参考

- ASDM配置指南
- 每个型号的Cisco ASA和ASDM兼容性

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。