Resolución de problemas de seguridad, certificados y vulnerabilidad de ASDM TLS

Contenido

Introducción

Este documento describe el proceso de solución de problemas de seguridad, certificados y vulnerabilidad de ASDM Transport Layer Security (TLS).

Background

El documento forma parte de la serie de solución de problemas del Administrador de dispositivos de seguridad adaptable (ASDM) junto con estos documentos:

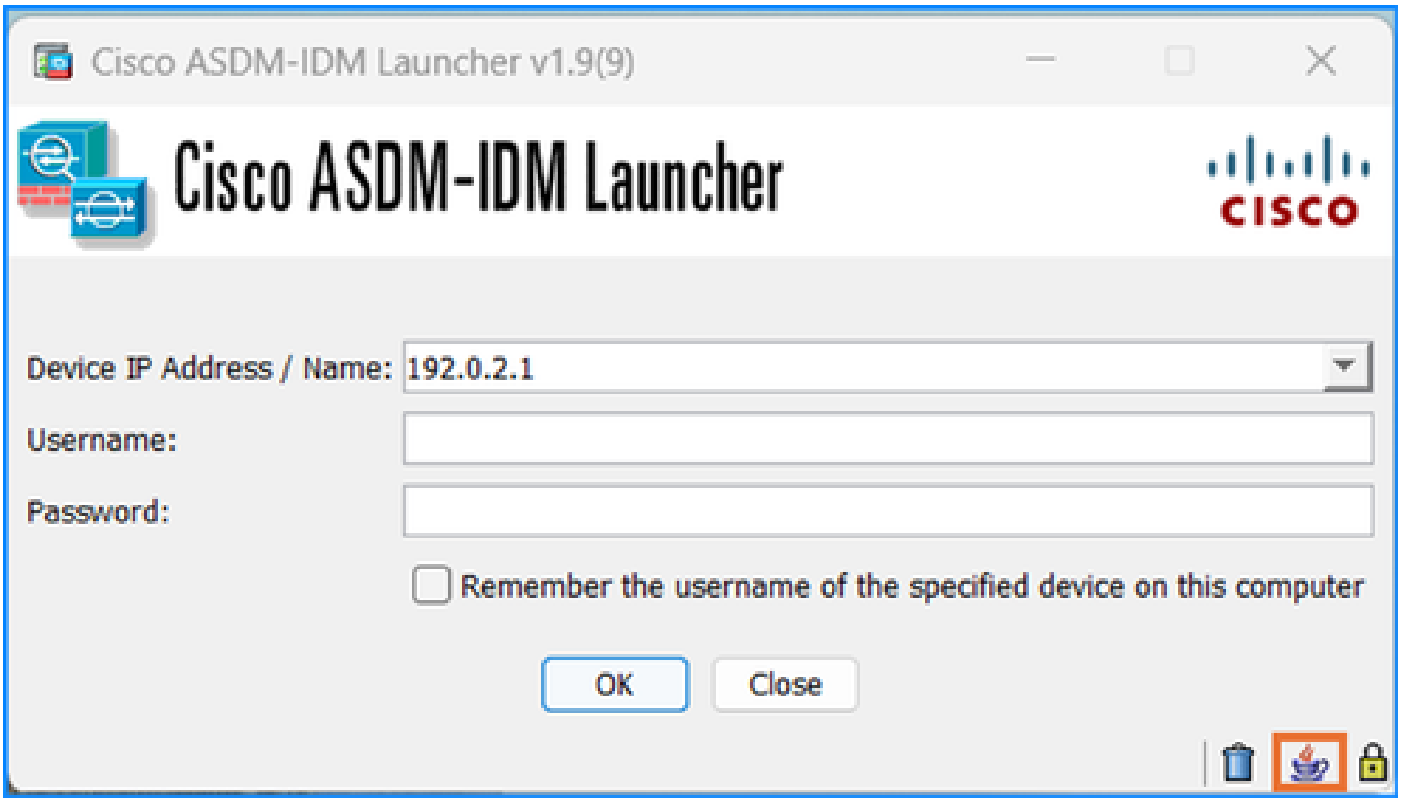
- Solucionar problemas de inicio de ASDM
- Resolución de Problemas de Configuración, Autenticación y Otros Problemas de ASDM
- Solución de problemas de licencia, actualización y compatibilidad de ASDM

Problemas de Cifrado TLS ASDM

Problema 1. ASDM no puede conectarse al firewall debido a problemas de cifrado TLS

ASDM no se puede conectar al firewall. Se observan uno o más de estos síntomas:

- ASDM muestra los mensajes de error "No se pudo abrir el dispositivo" o "No se puede iniciar el administrador de dispositivos desde <ip>".
- La salida del comando show ssl error contiene el error "SSL lib. Función: ssl3_get_client_hello Motivo: no shared cipher" message.
- Los registros de la consola Java muestran la excepción "javax.net.ssl.SSLHandshakeException: Alerta fatal recibida: mensaje de error 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)
```

Solución de problemas: acciones recomendadas

Una causa común de raíz de los síntomas es la falla de negociación del conjunto de cifrado TLS entre el ASDM y el ASA. En estos casos, dependiendo de la configuración de cifrado, el usuario necesita ajustar el certificado en el lado de ASMD y/o ASA.

Siga uno o más de estos pasos hasta que la conectividad sea exitosa:

1. En el caso de ASDM con OpenJRE si se utilizan conjuntos de cifrado TLS fuertes, aplique la solución alternativa del ID de error de software Cisco CSCvv12542 "ASDM open JRE debería utilizar cifrados más altos de forma predeterminada":
2. Iniciar el Bloc de notas (ejecutar como administrador)
3. Abra el archivo: C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security
4. Buscar por: crypto.policy=unlimited
5. Quite # delante de esa línea para que todas las opciones de cifrado estén disponibles
6. Guardar

2. Cambie los conjuntos de cifrado TLS en 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
```

Las opciones de cifrado para TLSv1.2:

<#root>

```
ASA(config)#
```

ssl cipher tlsv1.2 ?

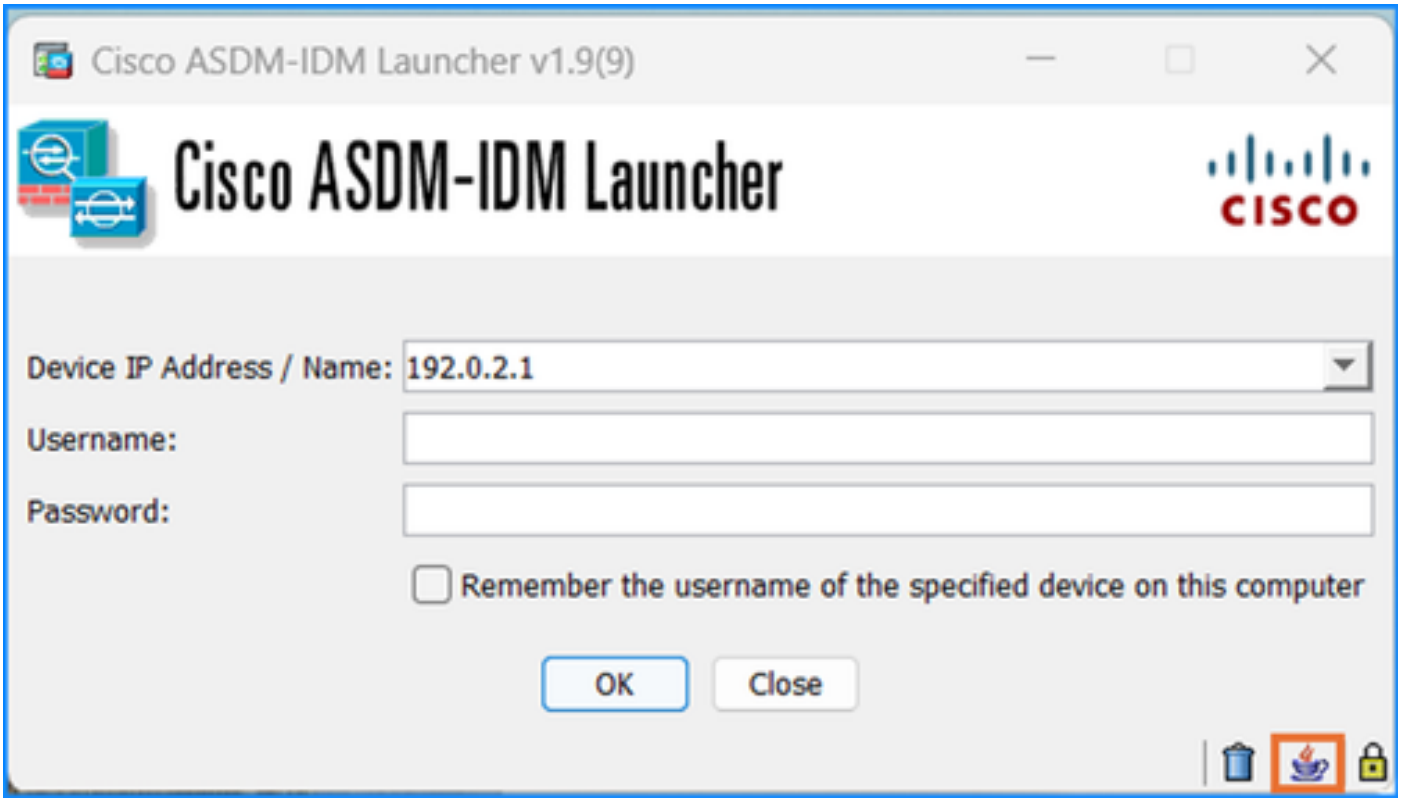
```
configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration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

Advertencia: Los cambios en el comando ssl cipher se aplican a todo el firewall, incluidas las conexiones VPN de sitio a sitio o de acceso remoto.

Problema 2. ASDM no se puede conectar a debido a una falla de intercambio de señales TLS1.3

El ASDM no puede conectarse a debido a una falla de intercambio de señales TLS1.3.

Los registros de la consola Java muestran la "java.lang.IllegalArgumentException: Mensaje de error de TLSv1.3":



<#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)
```

Solución de problemas: acciones recomendadas

La versión 1.3 de TLS debe ser compatible tanto con ASA como con ASDM. La versión 1.3 de TLS es compatible con las versiones 9.19.1 y posteriores de ASA (Release Notes para la serie ASA de Cisco Secure Firewall, 9.19(x)). Se necesita Oracle Java versión 8u261 o posterior para admitir TLS versión 1.3 (Release Notes para Cisco Secure Firewall ASDM, 7.19(x)).

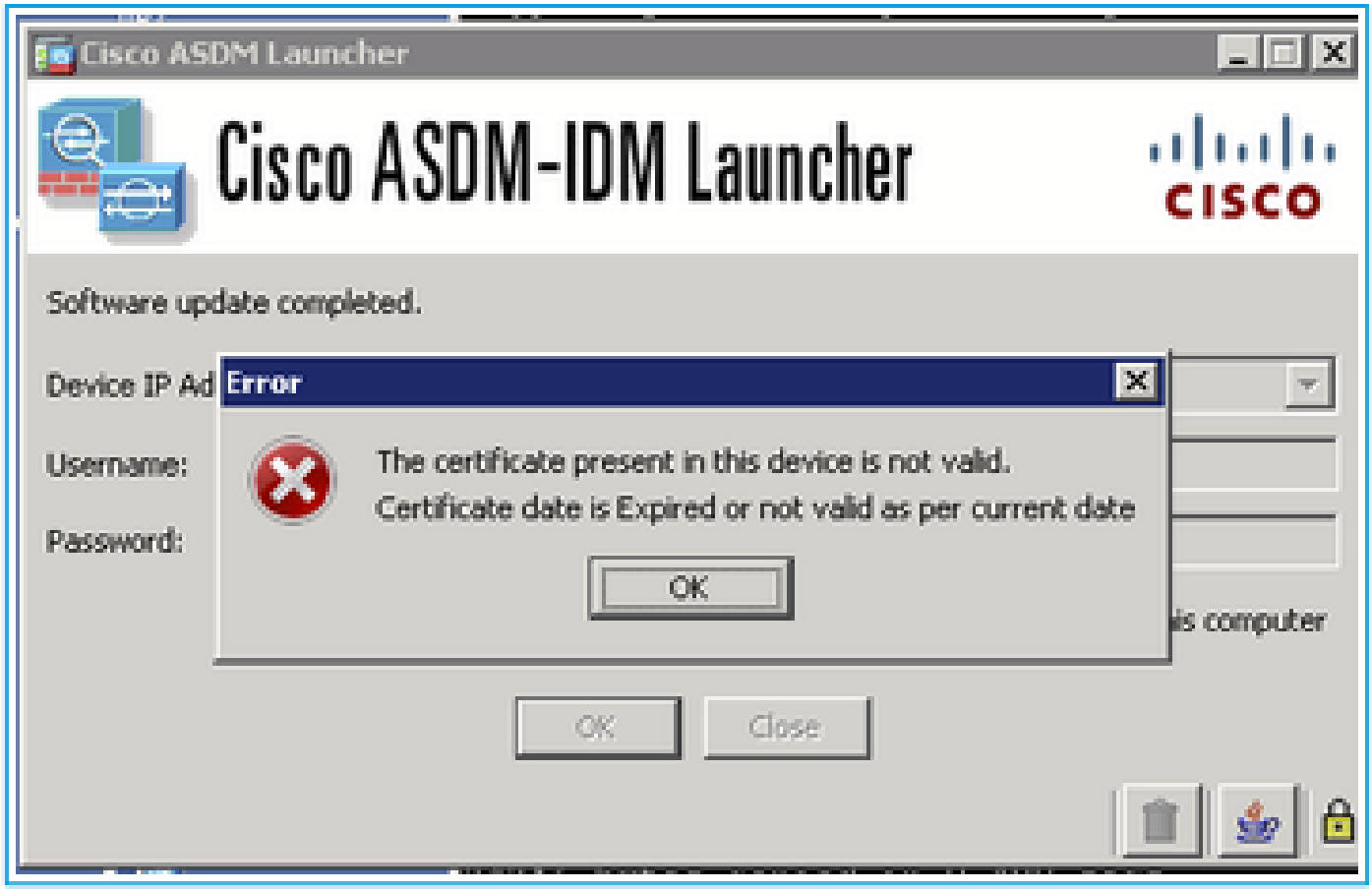
Referencias

1. Notas de la versión de Cisco Secure Firewall ASA Series, 9.19(x)
2. Notas de la versión de Cisco Secure Firewall ASDM, 7.19(x)

Problemas de certificado de ASDM

Problema 1. "El certificado presente en este dispositivo no es válido. La fecha del certificado ha caducado o no es válida según las fechas actuales." mensaje de error

El mensaje de error se muestra cuando se ejecuta ASDM: "El certificado presente en este dispositivo no es válido. La fecha del certificado ha caducado o no es válida según las fechas actuales."



Síntomas similares se describen en las notas de la versión:

"El certificado autofirmado de ASDM no es válido debido a una discordancia de fecha y hora con ASA. ASDM valida el certificado SSL autofirmado y, si la fecha de ASA no se encuentra dentro de la fecha de emisión y vencimiento del certificado, ASDM no se iniciará. Consulte Notas de compatibilidad de ASDM

Solución de problemas: acciones recomendadas

1. Comprobar y confirmar certificados caducados:

<#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. En la Interfaz de línea de comandos (CLI) de ASA, quite la línea ssl trust-point <cert> <interface>, donde <interface> es el nombre que se utiliza para las conexiones ASDM. El ASA utiliza certificado autofirmado para las conexiones ASDM.
2. Si no hay ningún certificado autofirmado, genere uno. En este ejemplo, el nombre SELF-SIGNED se utiliza como un nombre de punto verdadero:

<#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. Asocie el certificado generado con la interfaz:

<#root>

ssl trust-point SELF-SIGNED

4. Verifique el certificado:

<#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. Verifique la asociación del certificado con la interfaz:

<#root>

```
#
 show run all ssl
```

Problema 2. ¿Cómo instalar o renovar certificados mediante ASDM o ASA CLI?

Los usuarios desean aclarar los pasos para instalar o renovar certificados mediante ASDM o ASA CLI.

Acciones recomendadas

Consulte las guías para instalar y renovar certificados:

- ASA: Instalación y renovación del certificado digital de SSL
- Instalación y renovación de certificados en ASA administrados por CLI

Problemas de vulnerabilidad de ASDM

Esta sección trata los problemas más comunes relacionados con la vulnerabilidad de ASDM.

Problema 1. Vulnerabilidad detectada en ASDM

En caso de que detecte una vulnerabilidad en ASDM.

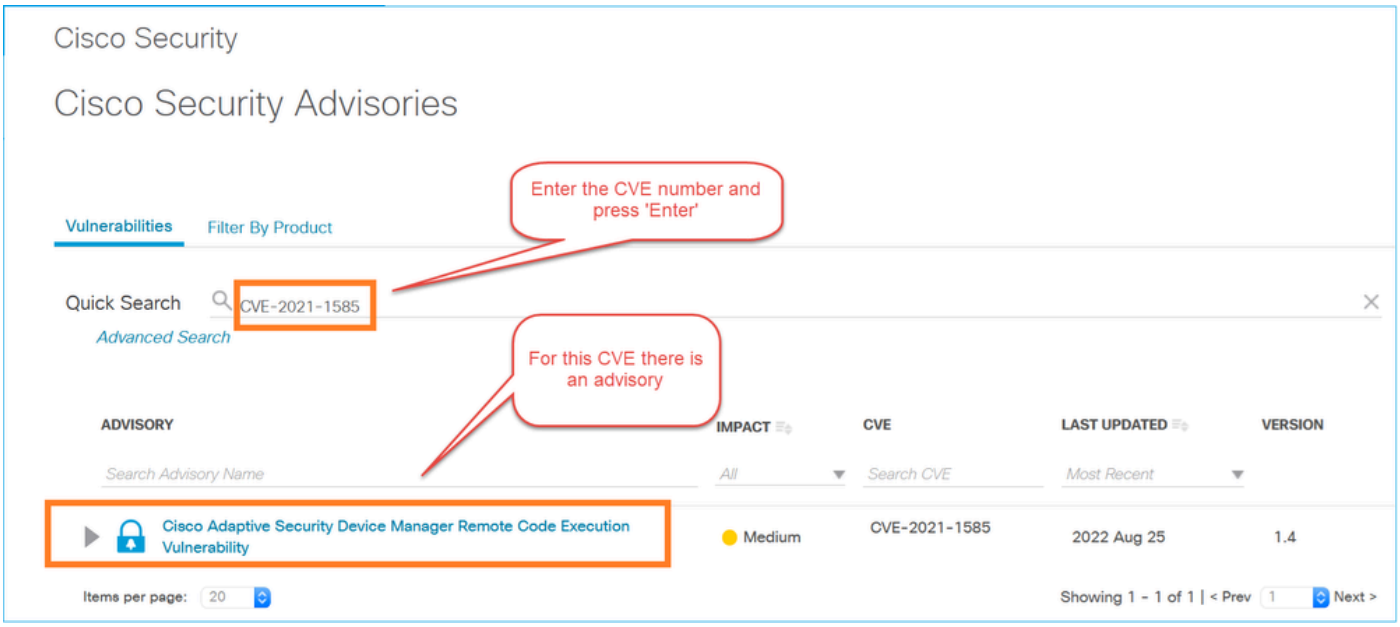
Solución de problemas: pasos recomendados

Paso 1: Identifique la ID de CVE (por ejemplo, CVE-2023-21930)

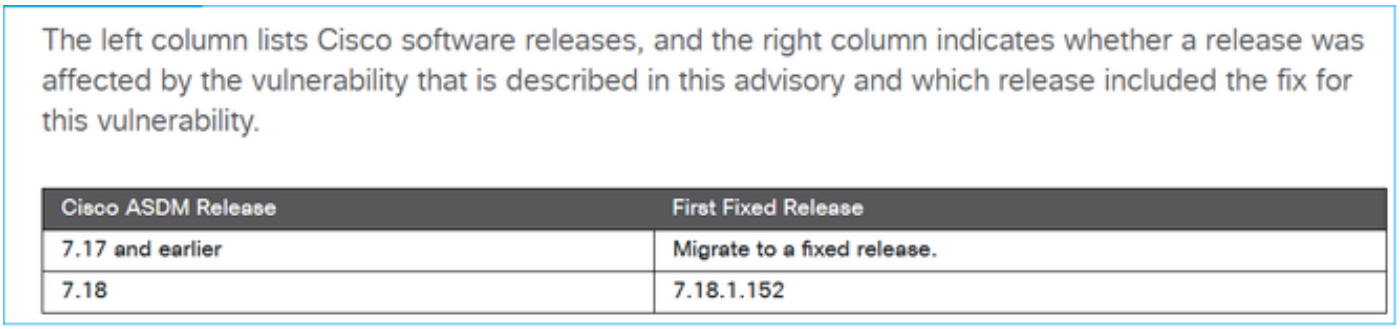
Paso 2: Busque CVE en las herramientas Cisco Security Advisories y Cisco Bug Search:

Acceda a la página de asesoramiento:

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



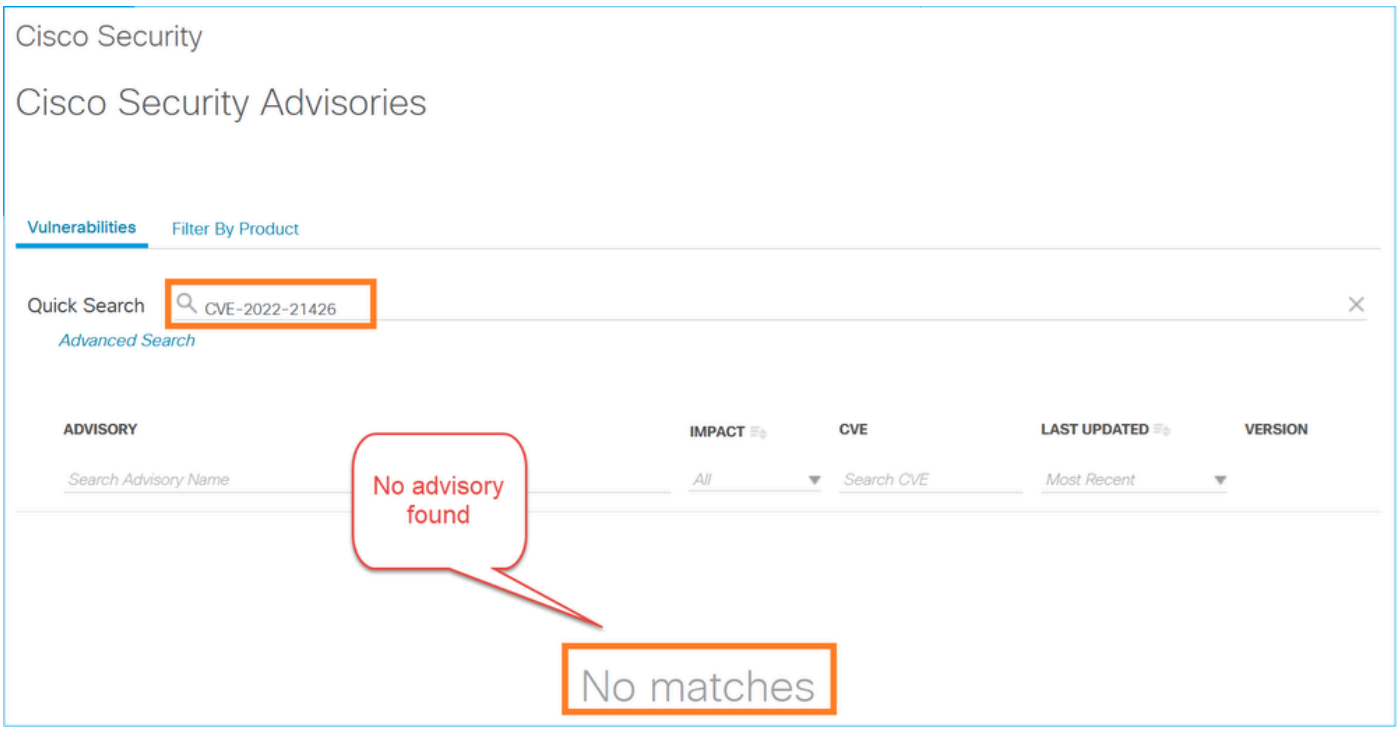
Abra el aviso y verifique si ASDM está afectado, por ejemplo:

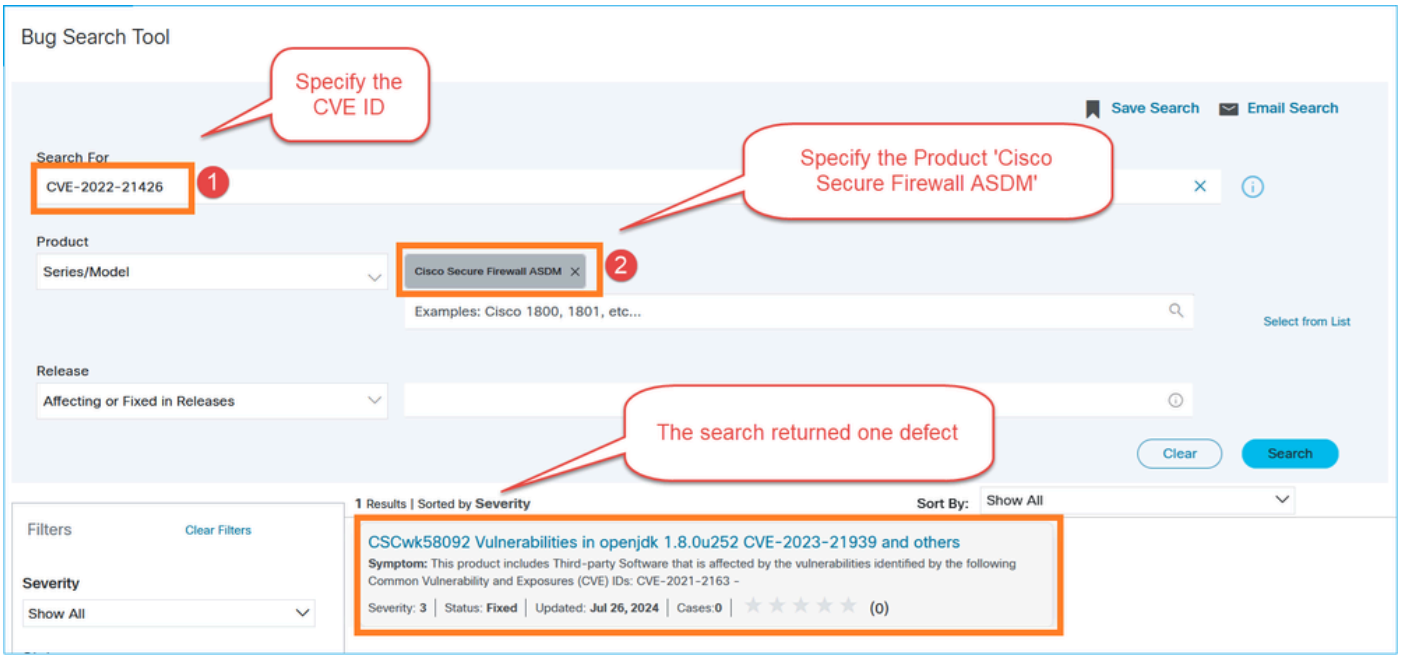


The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

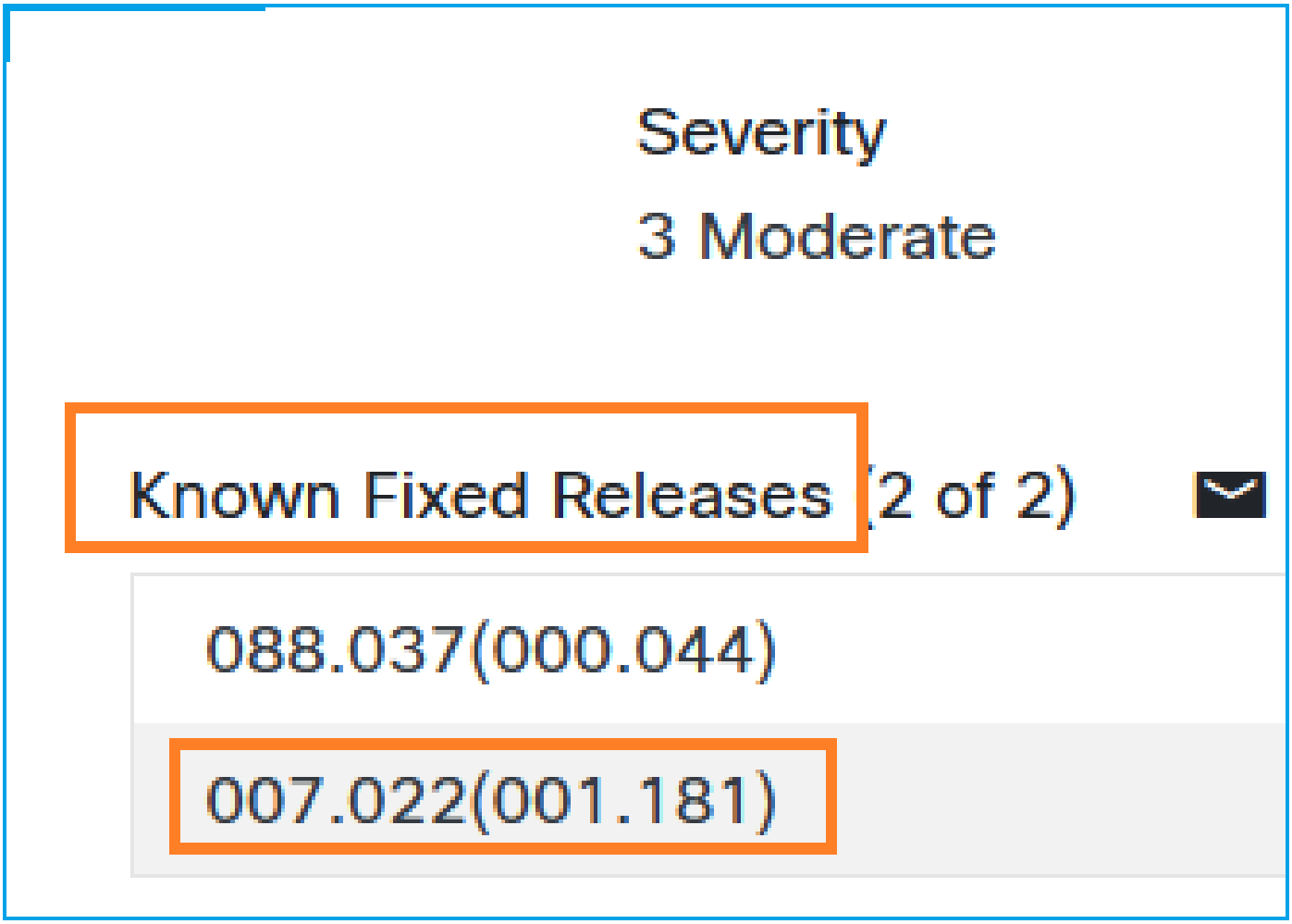
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

En caso de que no se encuentre ningún aviso, busque la ID de CVE en la herramienta de búsqueda de errores de Cisco (https://bst.cisco.com/bugsearch)





En este caso se identificó un defecto. Haga clic en él y compruebe sus detalles y la sección "Versiones fijas conocidas":



El defecto se corrige en la versión 7.22.1.181 del software ASDM.

Si las búsquedas en la herramienta de asesoramiento y en la herramienta de búsqueda de

errores para la ID de CVE especificada no han devuelto nada, debe trabajar con Cisco TAC para aclarar si ASDM se ve afectado por CVE.

Referencias

- Guías de Configuración de ASDM
- Compatibilidad de Cisco ASA y ASDM por modelo

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).