Dépannage des problèmes de sécurité, de certificat et de vulnérabilité ASDM TLS

Table des matières

Introduction

Ce document décrit la procédure de dépannage pour les problèmes de sécurité, de certificat et de vulnérabilité ASDM Transport Layer Security (TLS).

Fond

Ce document fait partie de la série de dépannages ASDM (Adaptive Security Appliance Device Manager), ainsi que les documents suivants :

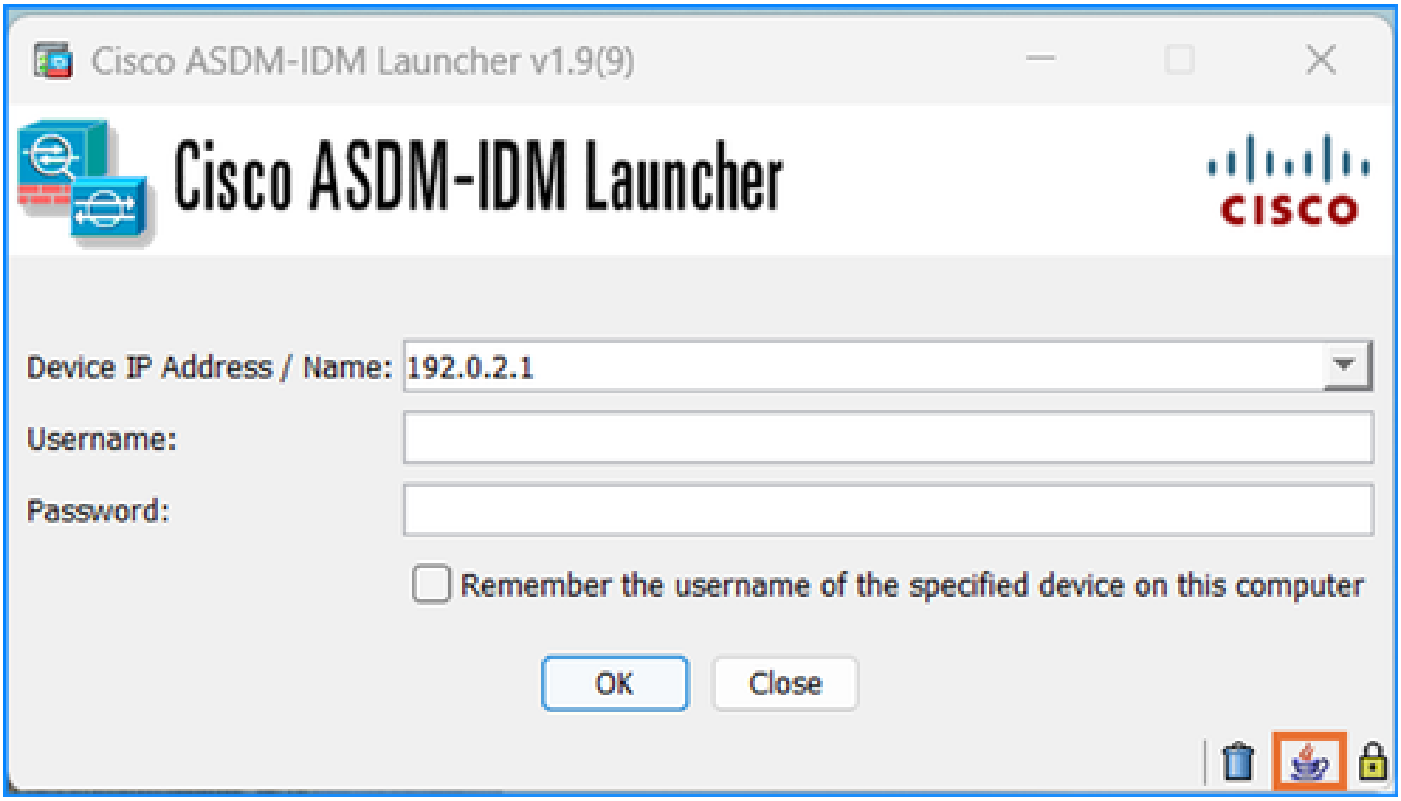
- Dépannage des problèmes de lancement ASDM
- Dépannage de la configuration, de l'authentification et d'autres problèmes ASDM
- Résoudre les problèmes de licence, de mise à niveau et de compatibilité ASDM

Problèmes de chiffrement TLS ASDM

Problème 1. ASDM ne peut pas se connecter au pare-feu en raison de problèmes de chiffrement TLS

ASDM ne peut pas se connecter au pare-feu. Un ou plusieurs des symptômes suivants sont observés :

- ASDM affiche les messages d'erreur « Could not open device » ou « Unable to launch device manager from <ip> ».
- Le résultat de la commande show ssl error contient l'erreur « SSL lib error. Fonction: ssl3_get_client_hello Motif : aucun message de chiffrement partagé ».
- Les journaux de la console Java affichent l'exception « javax.net.ssl.SSLHandshakeException : Alerte irrécupérable reçue : handshake_failure » message d'erreur :



<#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)
```

Dépannage - Actions recommandées

Une cause courante des symptômes est l'échec de la négociation de la suite de chiffrements TLS entre l'ASDM et l'ASA. Dans ces cas, en fonction de la configuration du chiffrement, l'utilisateur doit ajuster le certificat du côté ASMD et/ou ASA.

Effectuez une ou plusieurs des étapes suivantes jusqu'à ce que la connectivité soit établie :

1. Dans le cas d'ASDM avec OpenJRE si des suites de chiffrement TLS fortes sont utilisées, appliquez la solution de contournement du logiciel Cisco bug ID CSCv12542 « ASDM open JRE should use higher ciphers by default » :
2. Démarrer le Bloc-notes (en tant qu'administrateur)
3. Ouvrez le fichier : C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security
4. Rechercher : crypto.policy=illimité
5. Supprimez # devant cette ligne pour que toutes les options de cryptage soient disponibles
6. Enregistrer

2. Modifiez les suites de chiffrement TLS sur l'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
```

Options de chiffrement pour TLSv1.2 :

<#root>

```
ASA(config)#
```

ssl cipher tlsv1.2 ?

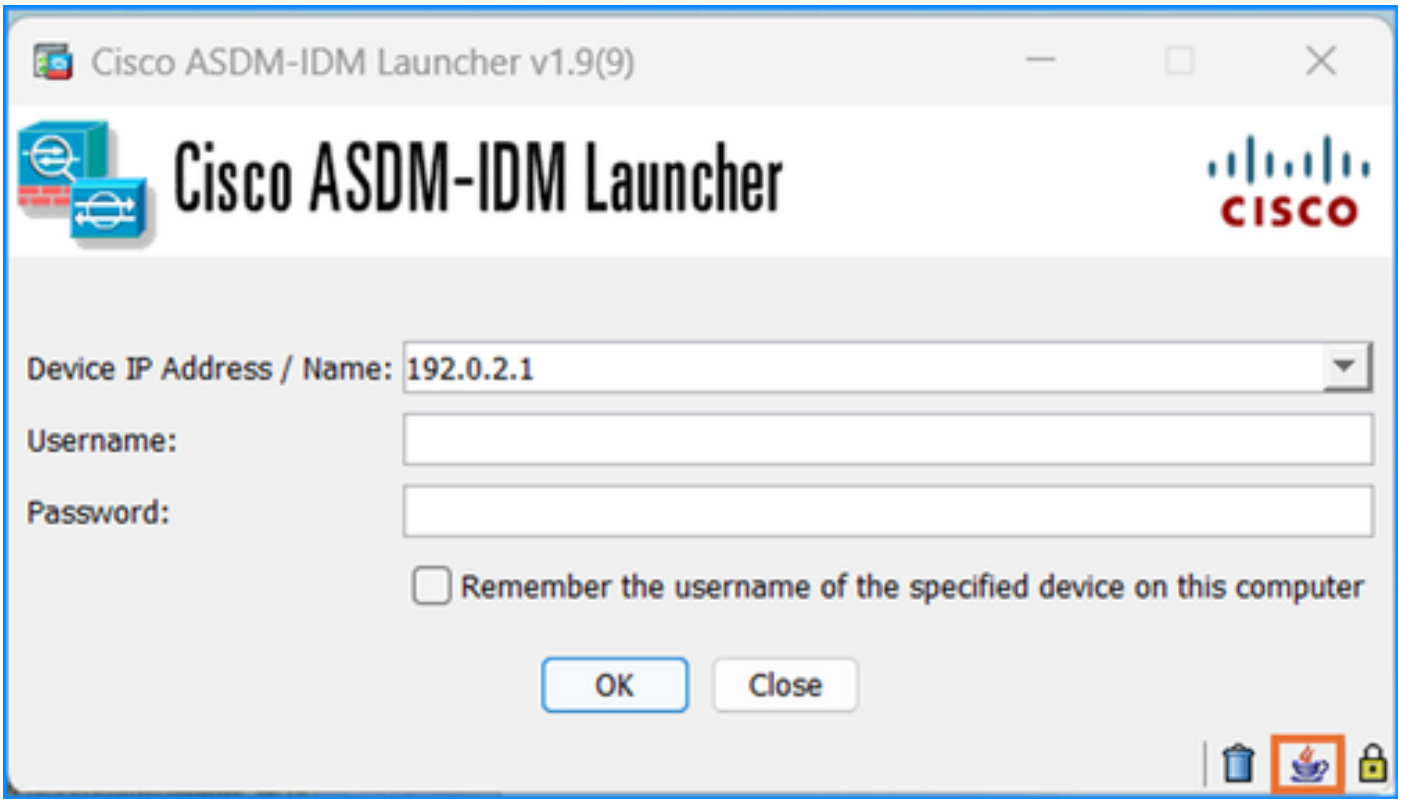
```
configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration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

Avertissement : Les modifications de la commande ssl cipher sont appliquées à l'ensemble du pare-feu, y compris les connexions VPN de site à site ou d'accès à distance.

Problème 2. L'ASDM ne peut pas se connecter à en raison d'un échec de connexion TLS1.3

L'ASDM ne peut pas se connecter à en raison d'un échec de connexion TLS1.3.

Les journaux de la console Java affichent « java.lang.IllegalArgumentException : Message d'erreur 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)
```

Dépannage - Actions recommandées

La version TLS 1.3 doit être prise en charge sur ASA et ASDM. TLS version 1.3 est pris en charge dans les versions 9.19.1 et ultérieures d'ASA (Notes de version pour la gamme Cisco

Secure Firewall ASA, 9.19(x)). Oracle Java version 8u261 ou ultérieure est requis pour prendre en charge TLS version 1.3 (Release Notes for Cisco Secure Firewall ASDM, 7.19(x)).

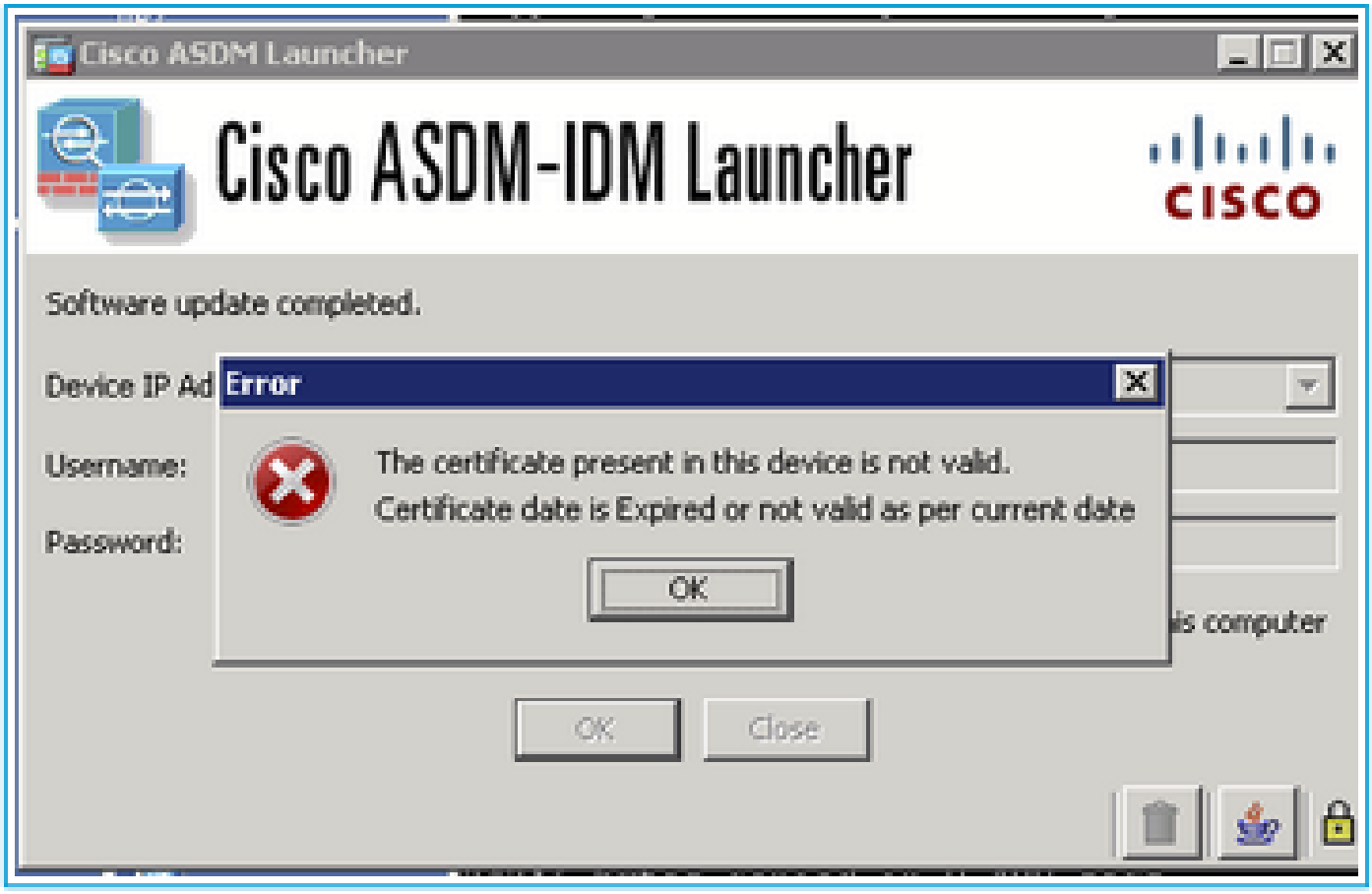
Références

1. Notes de version de la gamme Cisco Secure Firewall ASA, 9.19(x)
2. Notes de version de Cisco Secure Firewall ASDM, 7.19(x)

Problèmes de certificat ASDM

Problème 1. « Le certificat présent dans ce périphérique n'est pas valide. La date du certificat a expiré ou n'est pas valide selon les dates actuelles. »

Le message d'erreur suivant s'affiche lors de l'exécution d'ASDM : "Le certificat présent dans ce périphérique n'est pas valide. La date du certificat a expiré ou n'est pas valide selon les dates actuelles."



Des symptômes similaires sont décrits dans les notes de version :

« Le certificat auto-signé d'ASDM n'est pas valide en raison d'une incohérence d'heure et de date avec ASA : ASDM valide le certificat SSL auto-signé et si la date de l'ASA n'est pas comprise

dans la date d'émission le et d'expiration le du certificat, ASDM ne démarre pas. Voir Notes de compatibilité ASDM

Dépannage - Actions recommandées

1. Vérifiez et confirmez les certificats expirés :

<#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. Dans l'interface de ligne de commande ASA (CLI), supprimez la ligne ssl trust-point <cert> <interface>, où <interface> est le nom s'il est utilisé pour les connexions ASDM. ASA utilise

un certificat auto-signé pour les connexions ASDM.

2. S'il n'y a pas de certificat auto-signé, générez-en un. Dans cet exemple, le nom SELF-SIGNED est utilisé comme un vrai nom de point :

<#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. Associez le certificat généré à l'interface :

<#root>

ssl trust-point SELF-SIGNED

4. Vérifiez le certificat :

<#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. Vérifiez l'association du certificat avec l'interface :

<#root>

#

```
show run all ssl
```

Problème 2. Comment installer ou renouveler des certificats à l’aide de l’interface de ligne de commande ASDM ou ASA ?

Les utilisateurs souhaitent clarifier les étapes d'installation ou de renouvellement des certificats à l'aide de l'interface CLI ASDM ou ASA.

Actions recommandées

Reportez-vous aux guides d'installation et de renouvellement des certificats :

- ASA : Installation et renouvellement du certificat numérique SSL
- Installer et renouveler des certificats sur ASA géré par CLI

Problèmes de vulnérabilité ASDM

Cette section traite des problèmes les plus courants liés aux vulnérabilités ASDM.

Problème 1. Vulnérabilité détectée sur l’ASDM

Si vous détectez une vulnérabilité sur l'ASDM.

Dépannage - Étapes recommandées

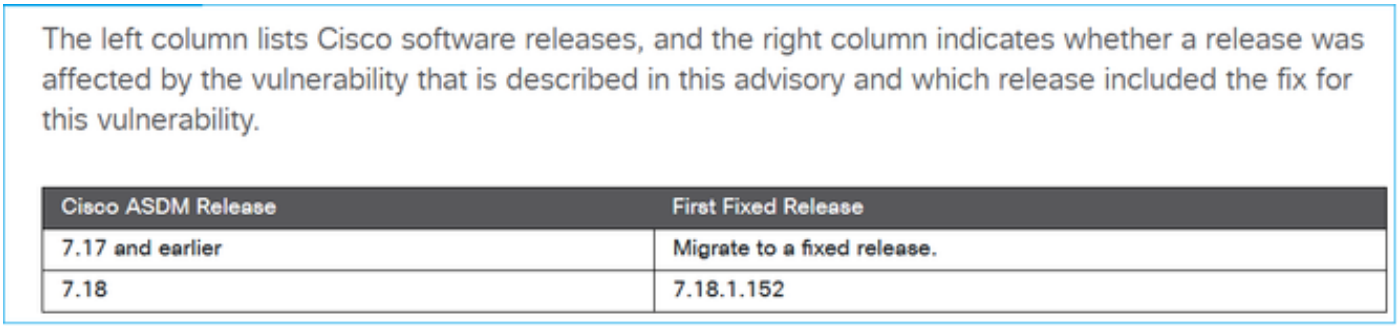
Étape 1 : Identifiez l'ID CVE (par exemple, CVE-2023-21930)

Étape 2 : Recherchez le CVE dans les avis de sécurité Cisco et dans l'outil de recherche de bogues Cisco :

Accédez à la page de conseil :

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

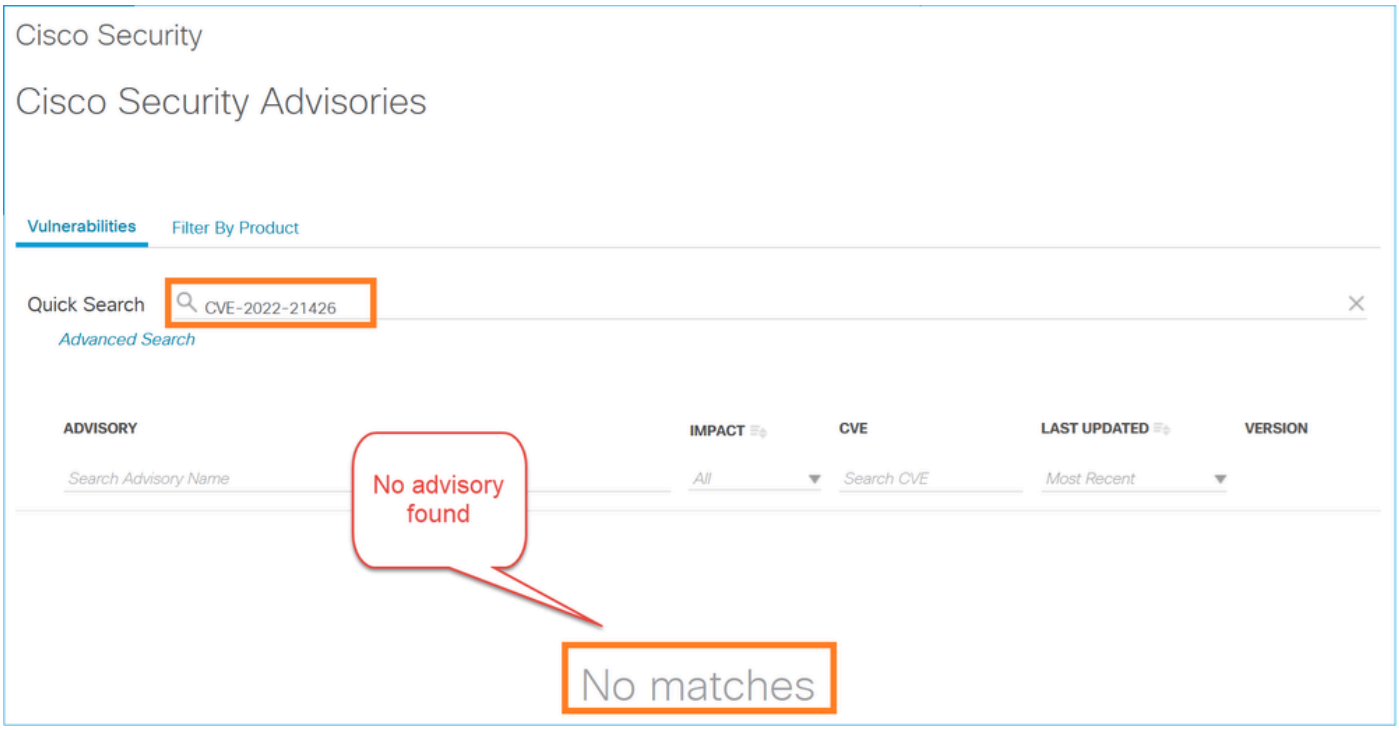
Ouvrez l'avis et vérifiez si l'ASDM est affecté, par exemple :

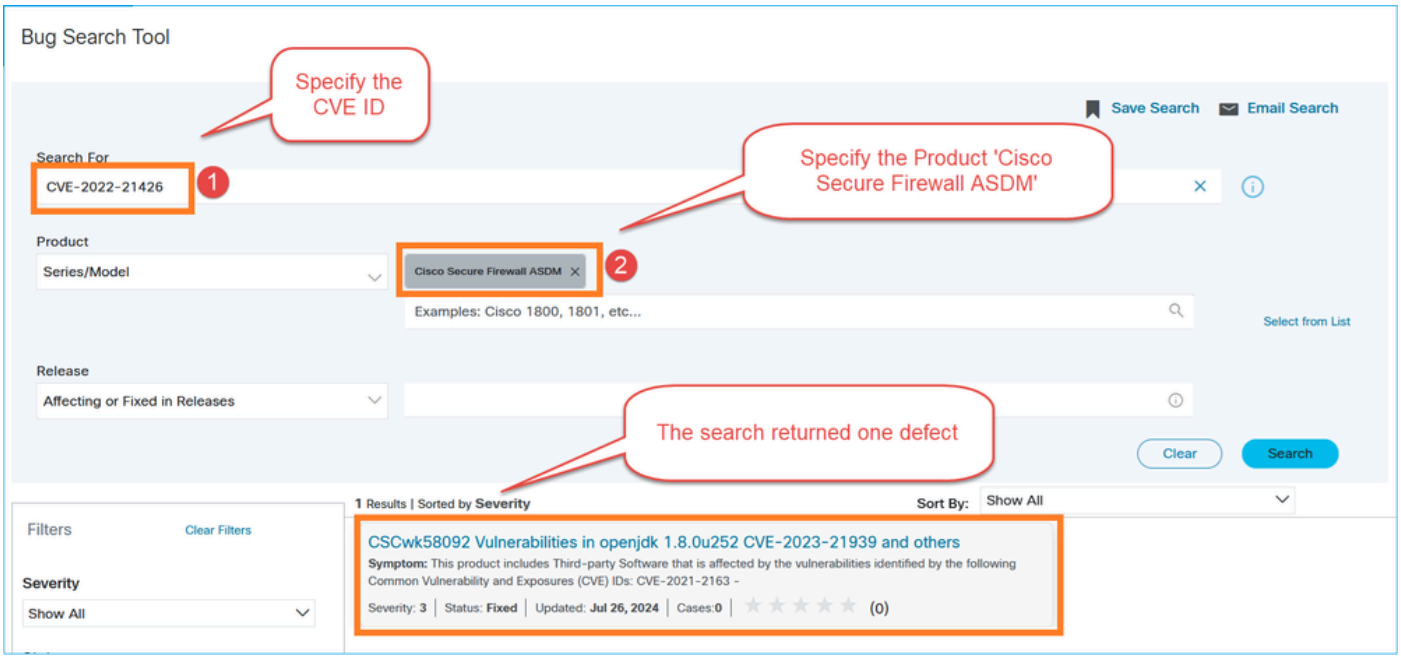


The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

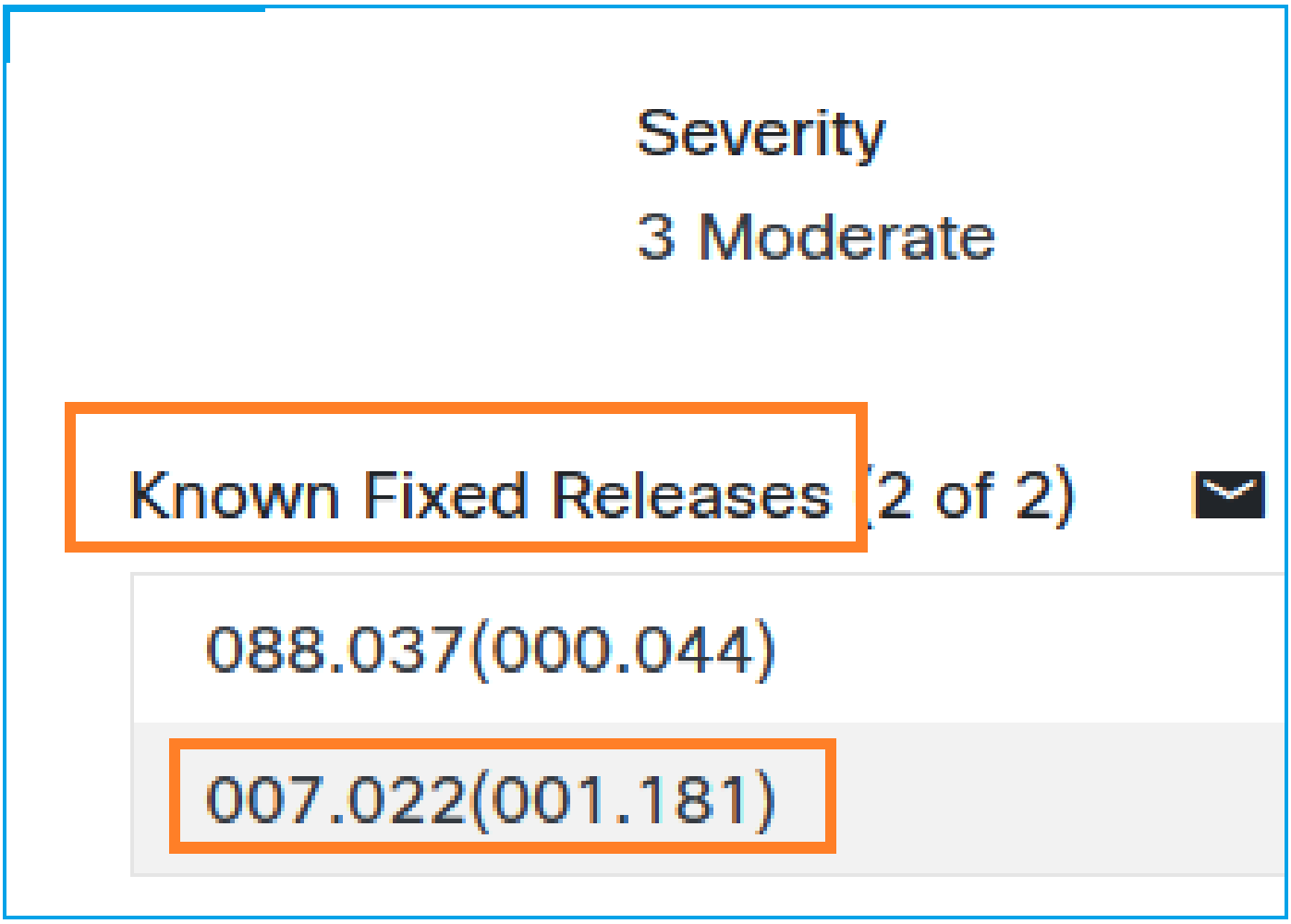
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

Si aucun conseil n'est trouvé, recherchez l'ID CVE dans l'outil de recherche de bogues Cisco (https://bst.cisco.com/bugsearch)





Dans ce cas, un défaut a été identifié. Cliquez dessus et vérifiez ses détails ainsi que la section « Known Fixed Releases » :



Le défaut est corrigé dans la version 7.22.1.181 du logiciel ASDM.

Si les recherches dans l'outil de conseil et l'outil de recherche de bogue pour l'ID CVE spécifié n'ont rien renvoyé, vous devez travailler avec le TAC Cisco pour clarifier si l'ASDM est affecté par le CVE.

Références

- Guides de configuration ASDM
- Compatibilité Cisco ASA et ASDM par modèle

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.