Risoluzione dei problemi di sicurezza, certificati e vulnerabilità di ASDM TLS

Sommario

Introduzione

In questo documento viene descritto il processo di risoluzione dei problemi di sicurezza, certificato e vulnerabilità di ASDM Transport Layer Security (TLS).

Introduzione

Il documento fa parte della serie ASDM (Adaptive Security Appliance Device Manager) per la risoluzione dei problemi, insieme ai seguenti documenti:

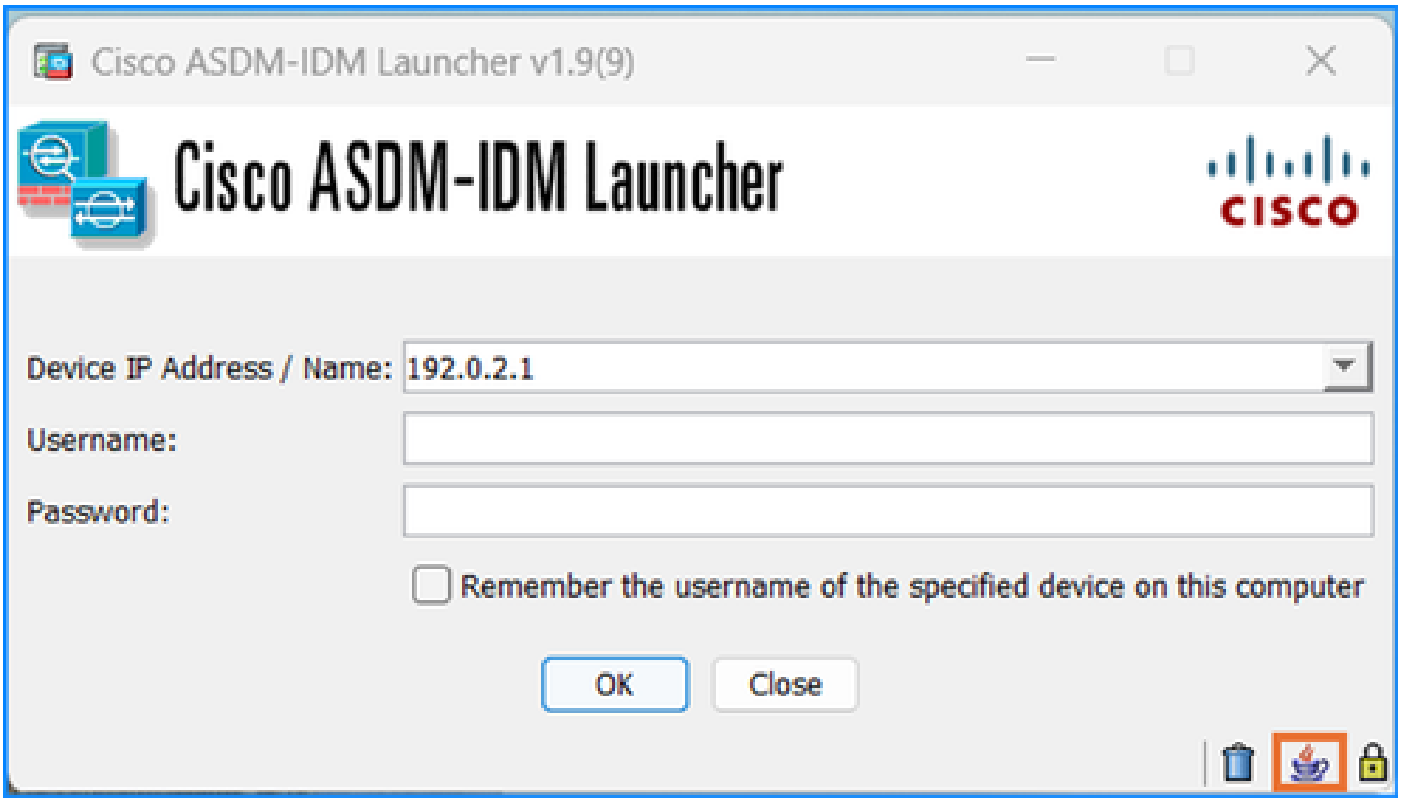
- Risoluzione dei problemi di avvio di ASDM
- Risoluzione dei problemi di configurazione, autenticazione e altri problemi di ASDM
- Risoluzione dei problemi relativi alle licenze ASDM, agli aggiornamenti e alla compatibilità

Problemi della crittografia ASDM TLS

Problema 1. ASDM non può connettersi al firewall a causa di problemi della cifratura TLS

ASDM non può connettersi al firewall. Si osservano uno o più dei seguenti sintomi:

- ASDM visualizza i messaggi di errore "Impossibile aprire il dispositivo" o "Impossibile avviare Gestione dispositivi da <ip>".
- L'output del comando show ssl error contiene l'errore "SSL lib error". Funzione: ssl3_get_client_hello Motivo: no shared cipher".
- Nei log della console Java viene visualizzato il messaggio "javax.net.ssl.SSLHandshakeException: È stato ricevuto un avviso di errore irreversibile: handshake_failure" messaggio di errore:



<#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)
```

Risoluzione dei problemi - Azioni consigliate

Una causa comune dei sintomi è il fallimento della negoziazione della suite di cifratura TLS tra ASDM e ASA. In questi casi, a seconda della configurazione della cifratura, l'utente deve modificare il certificato sull'appliance ASMD e/o sull'appliance ASA.

Eseguire uno o più dei seguenti passaggi fino al completamento della connettività:

1. Nel caso di ASDM con OpenJRE, se si usano suite di cifratura TLS avanzate, applicare la soluzione dal software Cisco bug ID CSCv12542 "ASDM open JRE should use high ciphers by default" (ASDM open JRE deve usare cifrature più alte per impostazione predefinita):
2. Avvia Blocco note (eseguito come amministratore)
3. Aprire il file: C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security
4. Cerca: crypto.policy=illimitato
5. Rimuovere # davanti alla riga in modo che tutte le opzioni di crittografia siano disponibili
6. Salva

2. Modificare le suite di cifratura TLS sull'appliance 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
```

Le opzioni di cifratura per TLSv1.2:

<#root>

```
ASA(config)#
```

ssl cipher tlsv1.2 ?

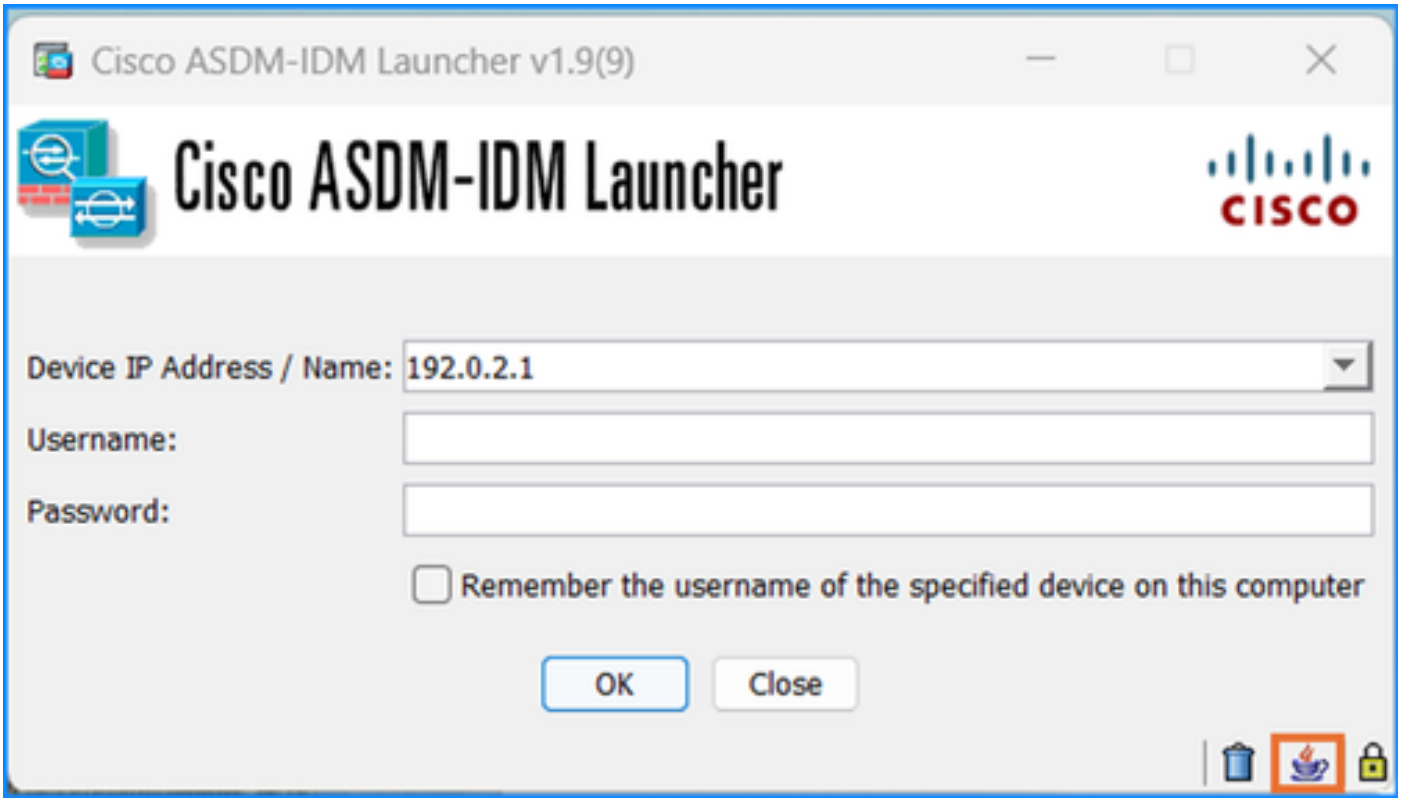
```
configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration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

Avviso: Le modifiche apportate al comando ssl cipher vengono applicate all'intero firewall, incluse le connessioni VPN da sito a sito o di accesso remoto.

Problema 2. Impossibile connettersi ad ASDM a causa di un errore dell'handshake TLS1.3

Impossibile connettersi ad ASDM a causa di un errore dell'handshake TLS1.3.

Nei log della console Java viene visualizzato il messaggio "java.lang.IllegalArgumentException: Messaggio di errore 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)
```

Risoluzione dei problemi - Azioni consigliate

La versione TLS 1.3 deve essere supportata sia su ASA che su ASDM. TLS versione 1.3 è supportato nelle versioni ASA 9.19.1 e successive (note di rilascio per Cisco Secure Firewall serie ASA, 9.19(x)). Per il supporto di TLS versione 1.3 (Note di rilascio per Cisco Secure Firewall ASDM, 7.19(x)), è richiesto Oracle Java versione 8u261 o successiva.

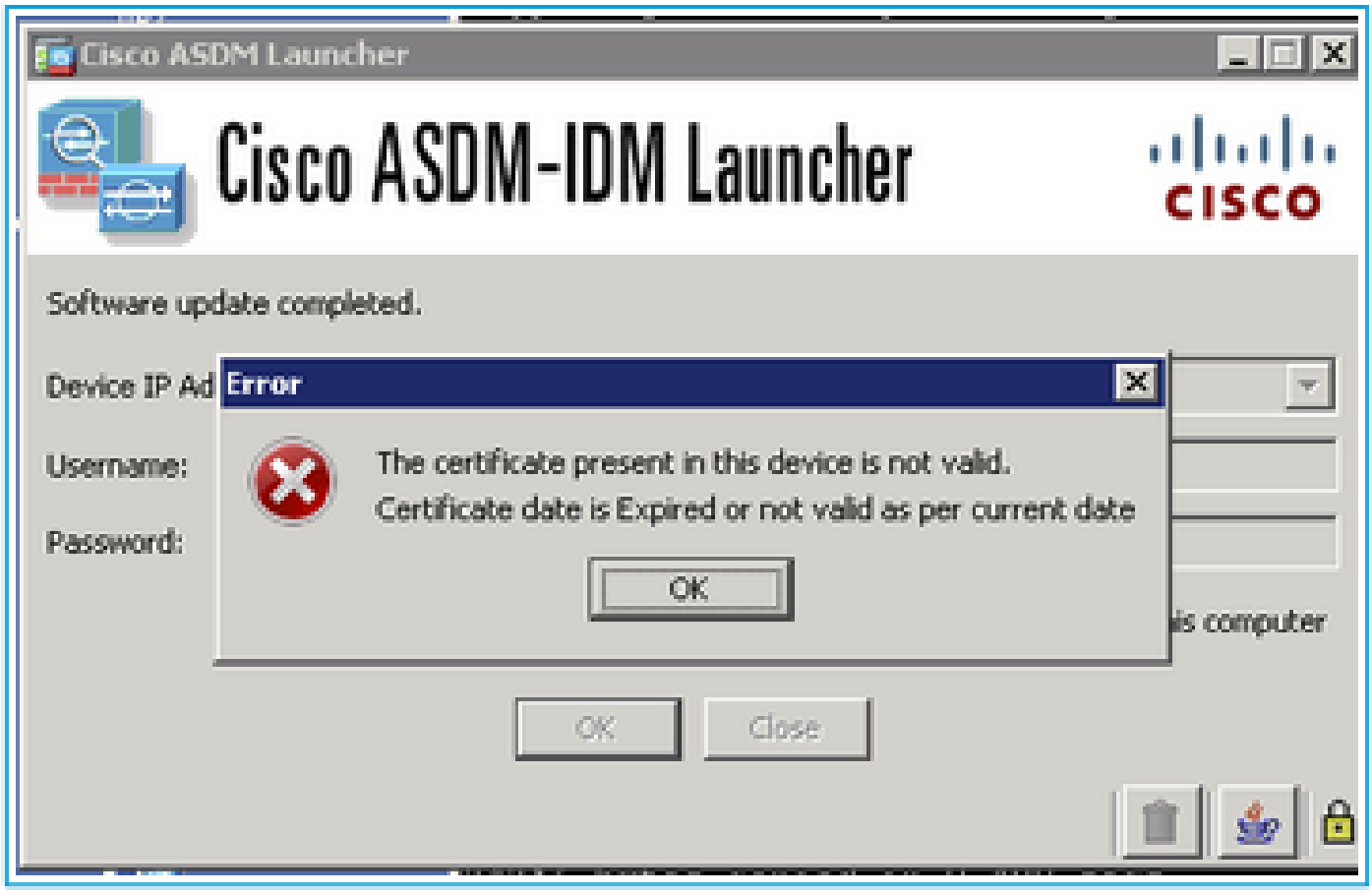
Riferimenti

1. Note sulla versione per Cisco Secure Firewall serie ASA, 9.19(x)
2. Note sulla versione di Cisco Secure Firewall ASDM, 7.19(x)

Problemi relativi ai certificati ASDM

Problema 1. "Il certificato presente nel dispositivo non è valido. La data del certificato è scaduta o non è valida come data corrente." Messaggio di errore

Quando si esegue ASDM viene visualizzato il messaggio di errore: "Il certificato presente nel dispositivo non è valido. La data del certificato è scaduta o non è valida come data corrente."



I sintomi simili sono descritti nelle note di rilascio:

"Il certificato autofirmato dell'ASDM non è valido a causa di una mancata corrispondenza di data e ora con l'ASA. ASDM convalida il certificato SSL autofirmato e, se la data dell'ASA non è compresa tra la data di emissione e la data di scadenza del certificato, ASDM non viene avviato. Vedere Note sulla compatibilità ASDM

Risoluzione dei problemi - Azioni consigliate

1. Verificare e confermare i certificati scaduti:

<#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. Nell'interfaccia della riga di comando (CLI) dell'ASA, rimuovere la riga ssl trust-point <cert> <interface>, dove <interface> è il nome utilizzato per le connessioni ASDM. L'appliance ASA utilizza un certificato autofirmato per le connessioni ASDM.
2. Se non è presente alcun certificato autofirmato, generarne uno. In questo esempio, il nome AUTOFIRMATO viene utilizzato come nome di punto vero:

<#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. Associare il certificato generato all'interfaccia:

<#root>

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

4. Verificare il certificato:

```
<#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. Verificare l'associazione del certificato all'interfaccia:

```
<#root>

#

 show run all ssl
```

Problema 2. Come installare o rinnovare i certificati utilizzando ASDM o ASA CLI?

Gli utenti desiderano specificare la procedura per installare o rinnovare i certificati utilizzando ASDM o ASA CLI.

Azioni consigliate

Fare riferimento alle guide per l'installazione e il rinnovo dei certificati:

- ASA: installazione e rinnovo del certificato digitale SSL
- Installazione e rinnovo dei certificati su un'appliance ASA gestita dalla CLI

Problemi di vulnerabilità ASDM

In questa sezione vengono illustrati i problemi più comuni di ASDM relativi alla vulnerabilità.

Problema 1. Vulnerabilità rilevata su ASDM

Se viene rilevata una vulnerabilità su ASDM.

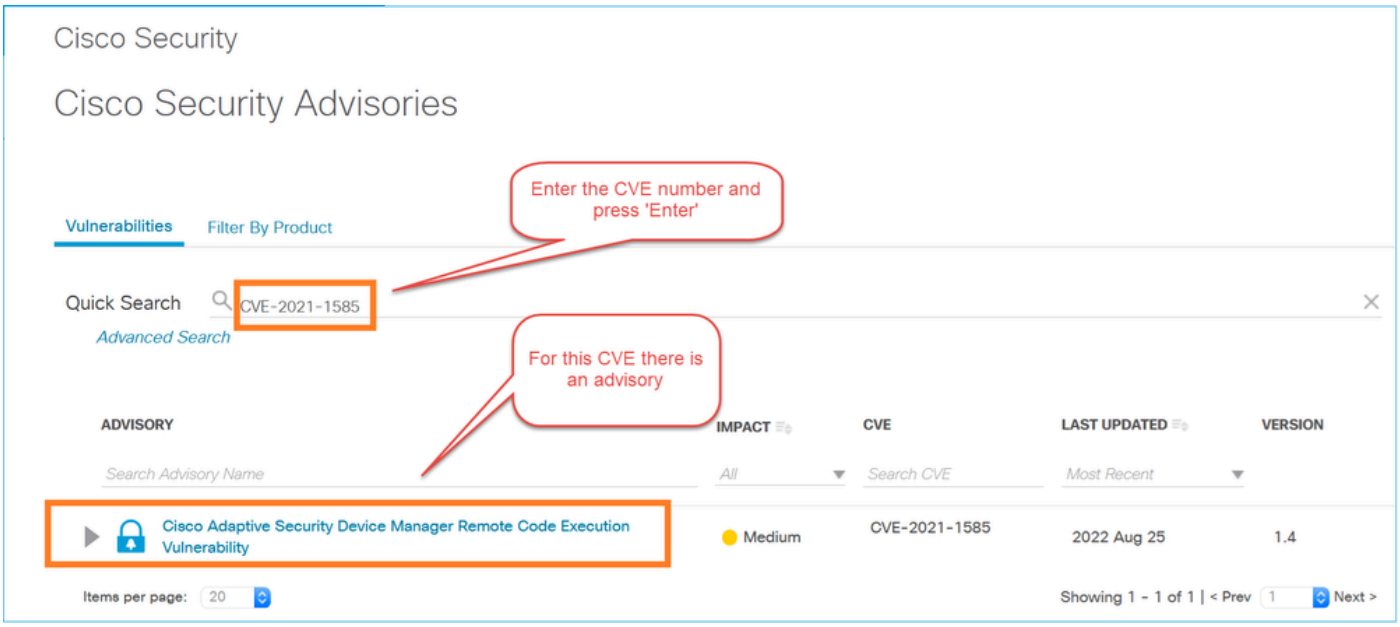
Risoluzione dei problemi - Passi consigliati

Passaggio 1: Identificare l'ID CVE (ad esempio, CVE-2023-21930)

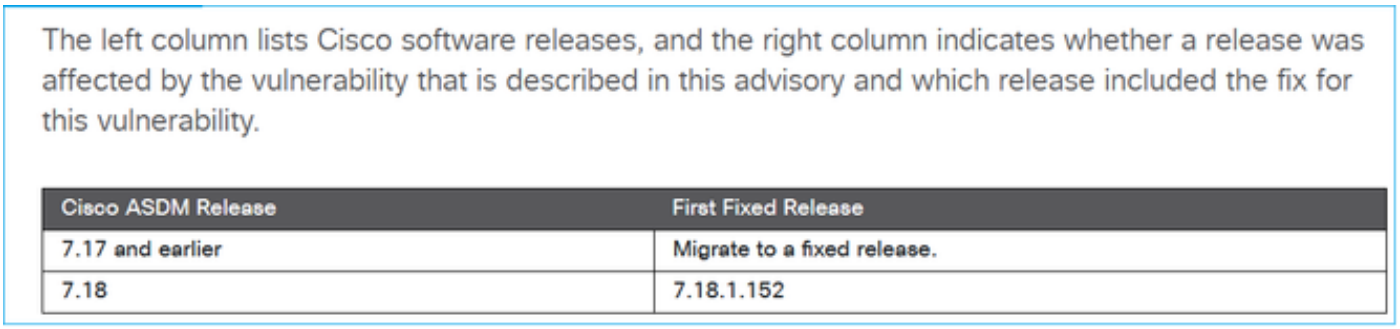
Passaggio 2: Cercare il CVE nei Cisco Security Advisories e Cisco Bug Search Tool:

Passare alla pagina advisory:

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



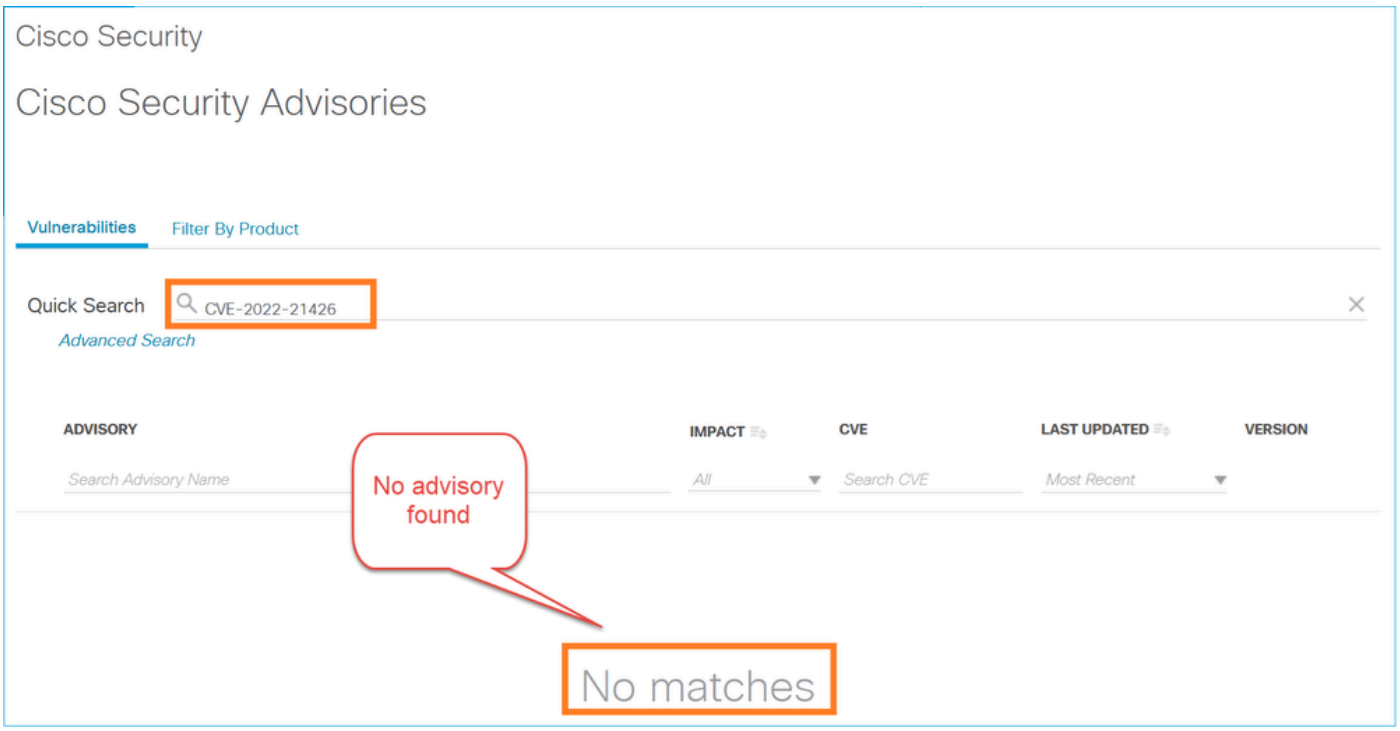
Aprire l'advisory e verificare se ASDM è interessato, ad esempio:

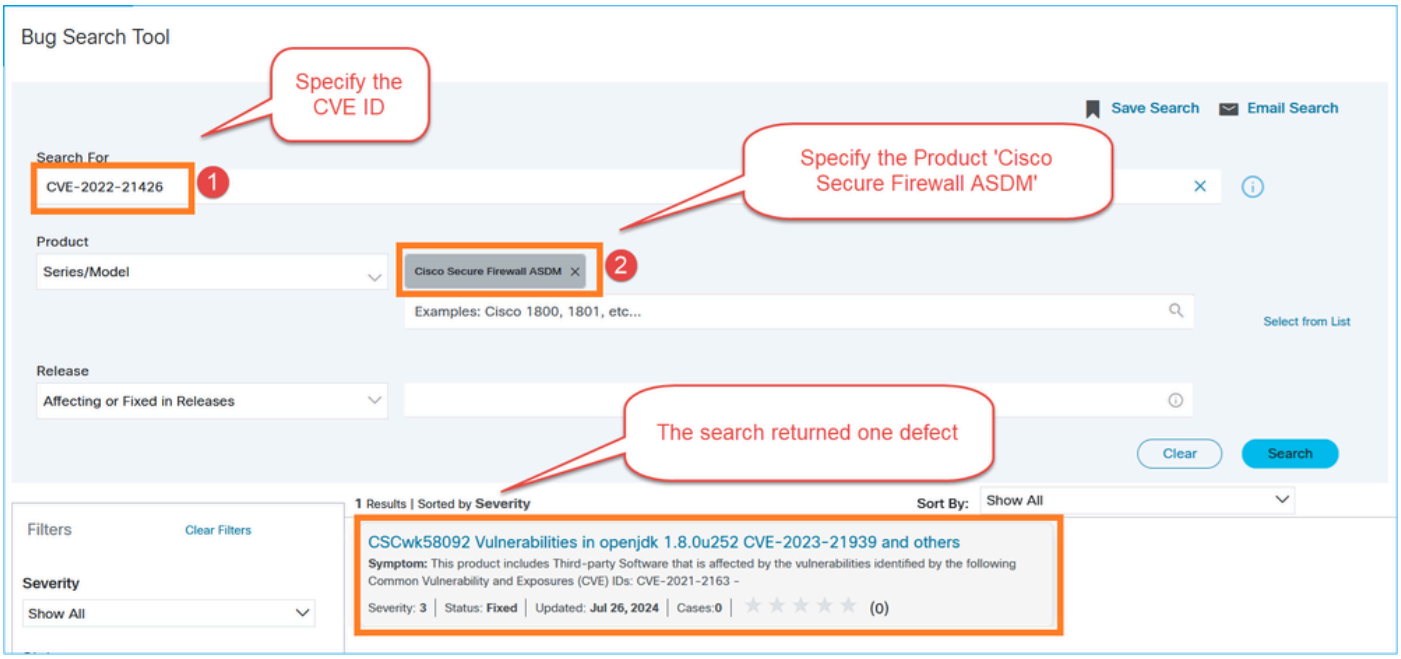


The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

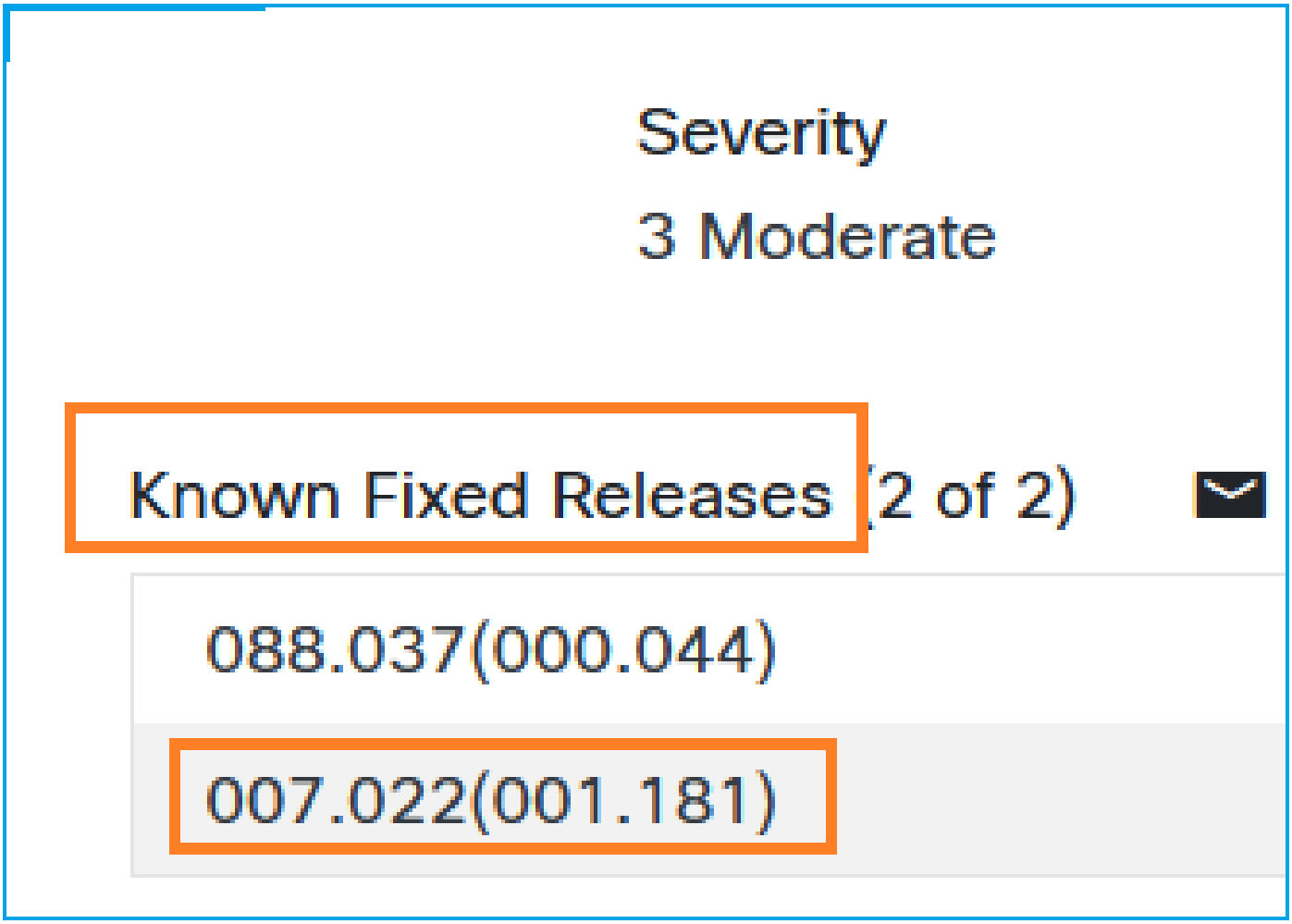
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

Se non viene trovato alcun avviso, cercare l'ID CVE in Cisco Bug Search Tool (https://bst.cisco.com/bugsearch)





In questo caso è stato identificato un difetto. Fare clic su di esso e controllare i suoi dettagli e la sezione 'Known Fixed Releases':



Il problema è stato risolto nella versione 7.2.1.181 del software ASDM.

se le ricerche nello strumento di consulenza e nello strumento di ricerca dei bug per l'ID CVE

specificato non hanno restituito nulla, è necessario lavorare con Cisco TAC per chiarire se ASDM è interessato dal CVE.

Riferimenti

- Guide alla configurazione ASDM
- Compatibilità Cisco ASA e ASDM per modello

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).