ASDM TLS 보안, 인증서 및 취약성 문제 해결

목차

소개

이 문서에서는 ASDM TLS(Transport Layer Security) 보안, 인증서 및 취약성 문제에 대한 트러블슈팅 프로세스에 대해 설명합니다.

배경

이 문서는 ASDM(Adaptive Security Appliance Device Manager) 문제 해결 시리즈의 일부이며 다음 문서와 함께 제공됩니다.

- ASDM 시작 문제 해결
- ASDM 컨피그레이션, 인증 및 기타 문제 해결
- ASDM 라이센스, 업그레이드 및 호환성 문제 해결

ASDM TLS 암호화 문제

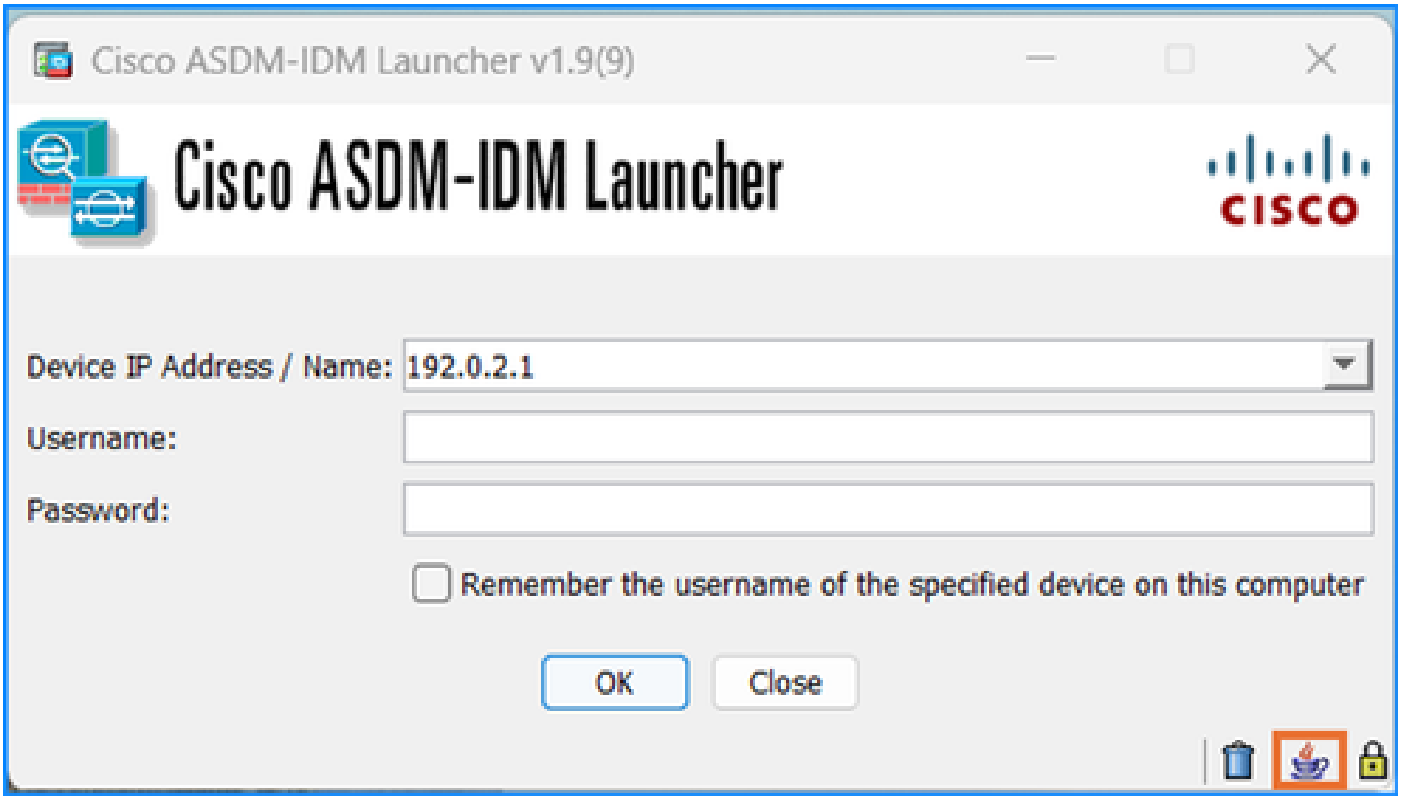
문제 1. TLS 암호화 문제로 인해 ASDM에서 방화벽에 연결할 수 없습니다.

ASDM에서 방화벽에 연결할 수 없습니다. 다음 증상 중 하나 이상이 관찰됩니다.

- ASDM에는 "Could not open device" 또는 "Unable to launch device manager from <ip>" 오류

메시지가 표시됩니다.

- show ssl error 명령의 출력에는 "SSL lib error"가 포함됩니다. 기능: ssl3_get_client_hello 이유: 공유 암호 없음" 메시지.
- Java 콘솔 로그에는 "javax.net.ssl.SSLHandshakeException이 표시됩니다. 치명적인 알림을 받았습니다. handshake_failure" 오류 메시지:



<#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)
```

문제 해결 - 권장 조치

증상의 일반적인 근본 원인은 ASDM과 ASA 간의 TLS 암호 그룹 협상 실패입니다. 이러한 경우 암호화 컨피그레이션에 따라 사용자는 ASMD 및/또는 ASA 측에서 인증서를 조정해야 합니다.

연결에 성공할 때까지 다음 단계 중 하나 이상을 수행합니다.

1. OpenJRE가 포함된 ASDM의 경우 강력한 TLS 암호 그룹을 사용하는 경우 소프트웨어 Cisco 버그 ID CSCv12542 "ASDM open JRE는 기본적으로 더 높은 암호를 사용해야 합니다."에서

해결 방법을 적용합니다.

2. 메모장 시작(관리자로 실행)
3. 파일을 엽니다. C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security
4. 검색 대상: crypto.policy=unlimited
5. 모든 암호화 옵션을 사용할 수 있도록 해당 줄 앞에 있는 #을 제거
6. 저장

2. ASA에서 TLS 암호 그룹을 변경합니다.

<#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
```

TLSv1.2의 암호화 옵션:

<#root>

```
ASA(config)#
```

ssl cipher tlsv1.2 ?

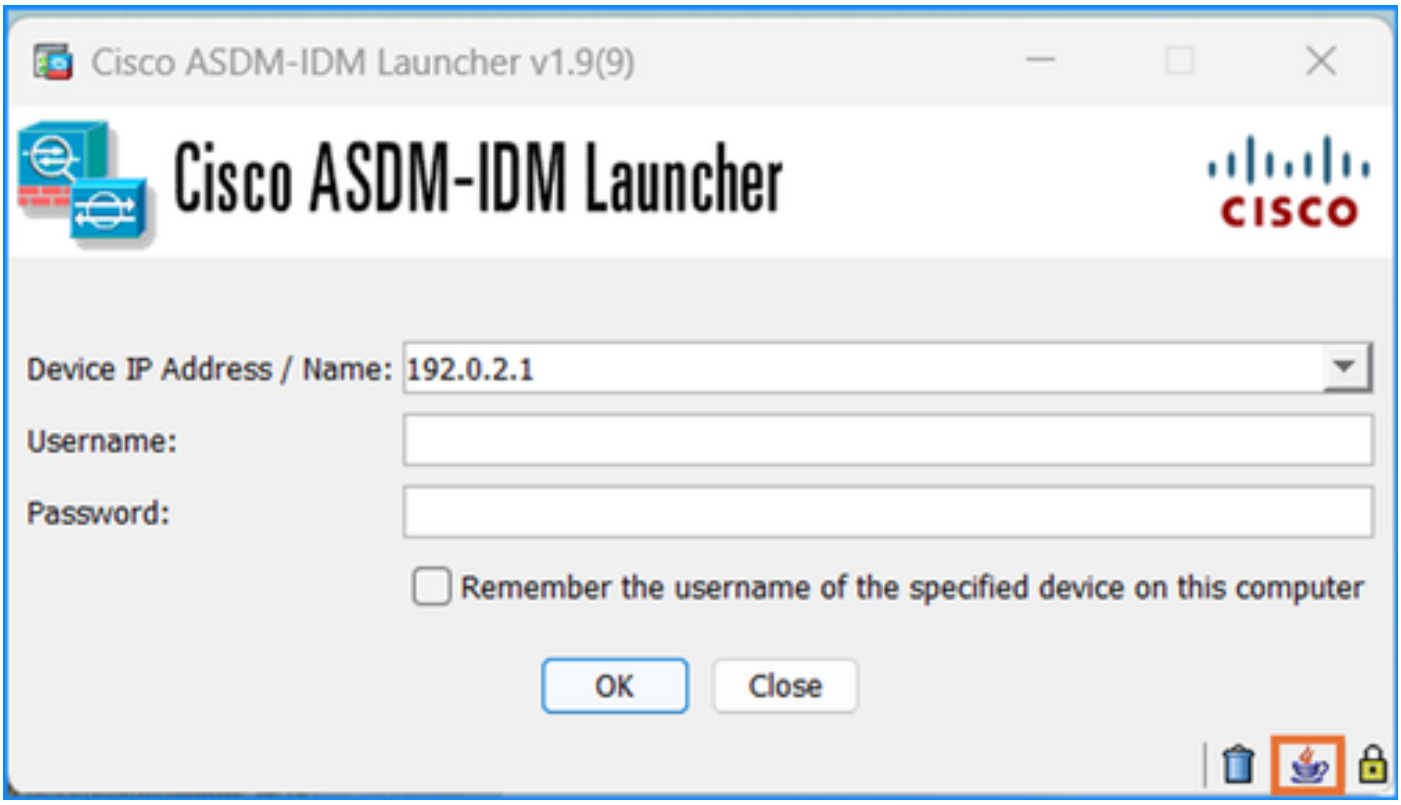
```
configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration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

경고: ssl cipher 명령의 변경 사항은 사이트 대 사이트 또는 원격 액세스 VPN 연결을 비롯한 전체 방화벽에 적용됩니다.

문제 2. TLS1.3 핸드셰이크 오류로 인해 ASDM에 연결할 수 없습니다.

TLS1.3 핸드셰이크 오류로 인해 ASDM에 연결할 수 없습니다.

Java 콘솔 로그에는 "java.lang.InlegatedArgumentException이 표시됩니다. TLSv1.3" 오류 메시지:



<#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)
```

문제 해결 - 권장 조치

TLS 1.3 버전은 ASA와 ASDM에서 모두 지원되어야 합니다. TLS 버전 1.3은 ASA 버전 9.19.1 이상에서 지원됩니다(Cisco Secure Firewall ASA Series 릴리스 정보, 9.19(x)). TLS 버전 1.3을 지원하려면 Oracle Java 버전 8u261 이상이 필요합니다(Cisco Secure Firewall ASDM 릴리스 정보, 7.19(x)).

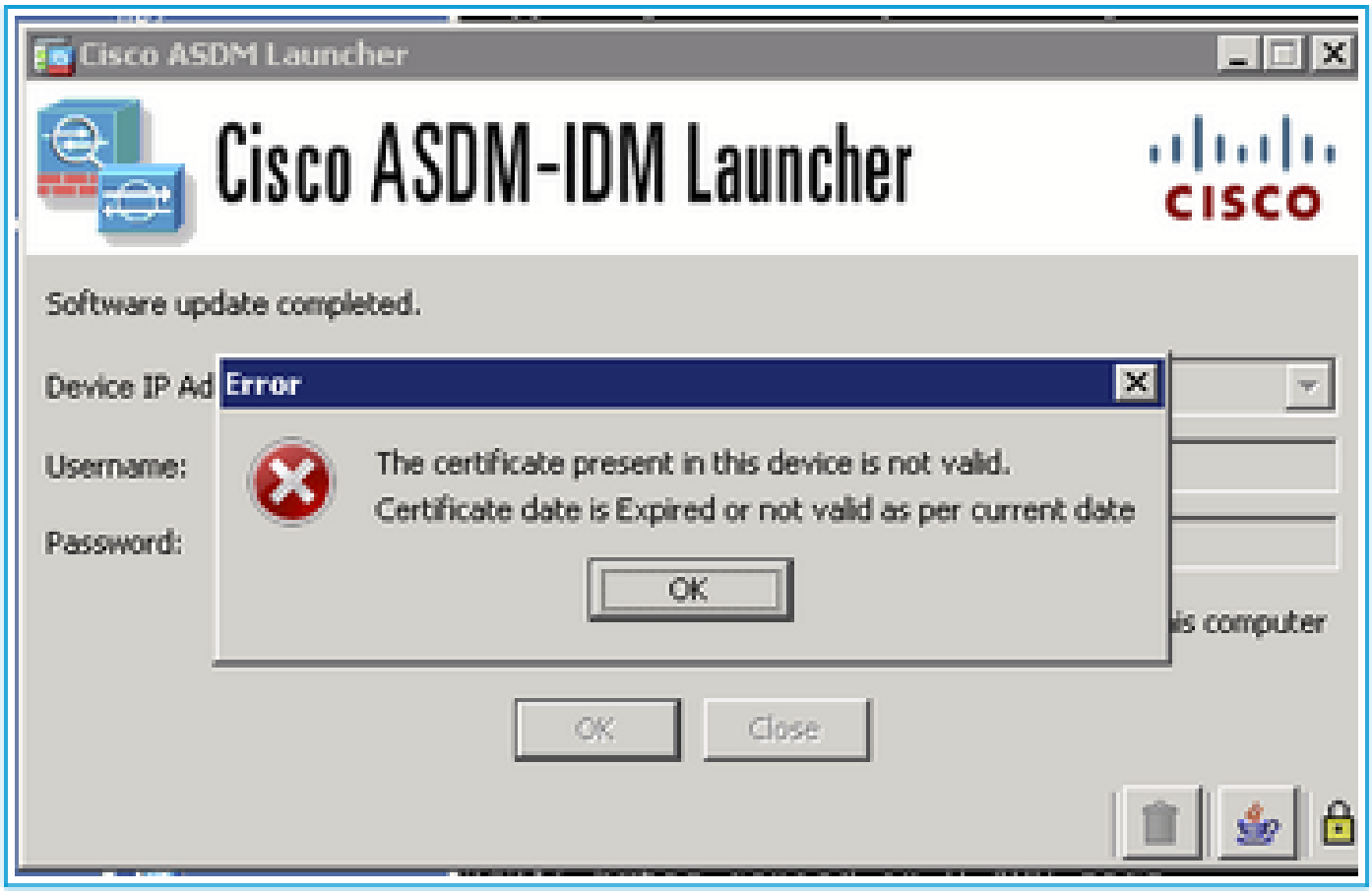
참조

1. Cisco Secure Firewall ASA Series 릴리스 정보, 9.19(x)
2. Cisco Secure Firewall ASDM 릴리스 정보, 7.19(x)

ASDM 인증서 문제

문제 1. "이 장치에 있는 인증서가 유효하지 않습니다. 인증서 날짜가 만료되었거나 현재 날짜로 유효하지 않습니다." 오류 메시지가 표시됩니다

ASDM을 실행하면 다음과 같은 오류 메시지가 표시됩니다. "이 장치에 있는 인증서가 유효하지 않습니다. 인증서 날짜가 만료되었거나 현재 날짜로 유효하지 않습니다."



유사한 증상은 릴리스 노트에 설명되어 있습니다.

"ASA와 시간 및 날짜가 일치하지 않아 ASDM의 자체 서명 인증서가 유효하지 않음 - ASDM은 자체 서명 SSL 인증서를 검증하며, ASA의 날짜가 인증서의 Issued On 및 Expires On 날짜 내에 있지 않으면 ASDM이 실행되지 않습니다. 참조 ASDM 호환성 참고 사항

문제 해결 - 권장 조치

1. 만료된 인증서 확인 및 확인:

<#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. ASA CLI(Command Line Interface)에서 ssl trust-point <cert> <interface>를 제거합니다. 여기서 <interface>는 ASDM 연결에 사용되는 nameif입니다. ASA는 ASDM 연결에 자체 서명 인증서를 사용합니다.
2. 자체 서명 인증서가 없는 경우 인증서를 생성합니다. 이 예에서 자체 서명 이름은 실제 포인트 이름으로 사용됩니다.

<#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. 생성된 인증서를 인터페이스와 연결합니다.

<#root>

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

4. 인증서를 확인합니다.

<#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. 인터페이스와의 인증서 연결을 확인합니다.

<#root>

#

show run all ssl

문제 2. ASDM 또는 ASA CLI를 사용하여 인증서를 설치하거나 갱신하는 방법

사용자는 ASDM 또는 ASA CLI를 사용하여 인증서를 설치하거나 갱신하는 단계를 명확히 하고자 합니다.

권장 작업

인증서를 설치 하고 업데이트 하려면 설명서를 참조 하십시오.

- ASA: SSL 디지털 인증서 설치 및 갱신
- CLI로 관리되는 ASA에 인증서 설치 및 갱신

ASDM 취약성 문제

이 섹션에서는 가장 일반적인 ASDM 취약성 관련 문제를 다룹니다.

문제 1. ASDM에서 탐지된 취약성

ASDM에서 취약성을 탐지하는 경우.

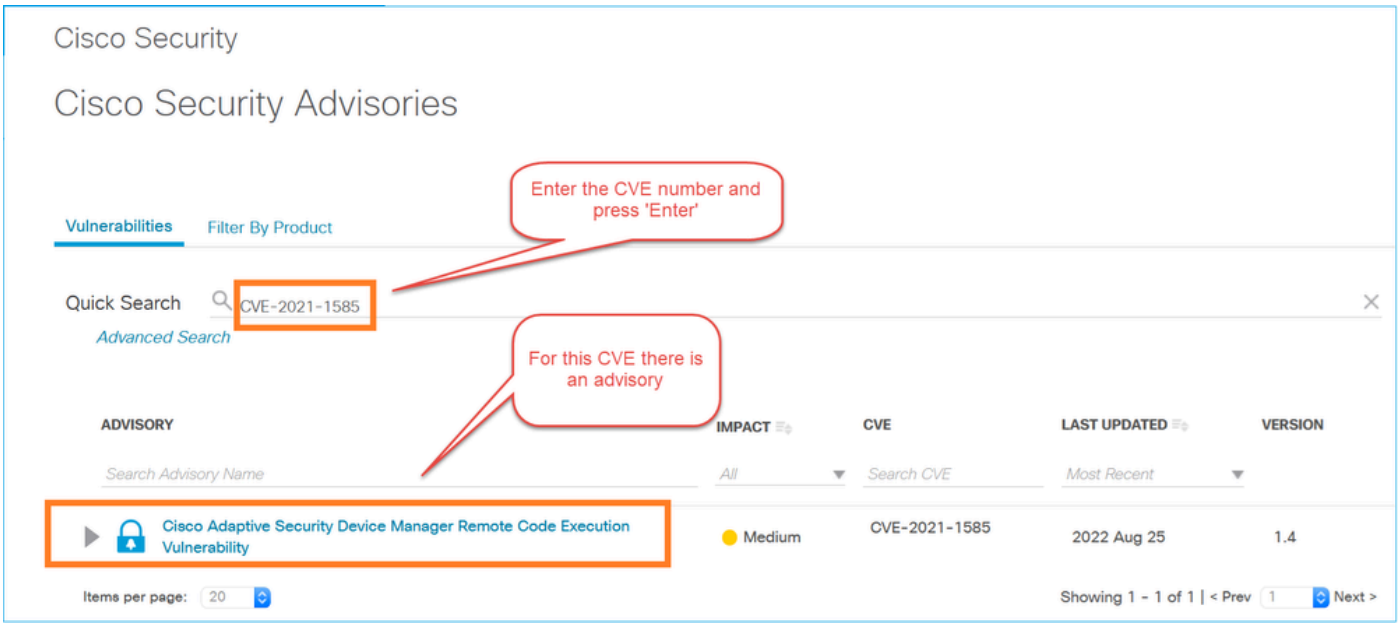
문제 해결 - 권장 단계

1단계: CVE ID 식별(예: CVE-2023-21930)

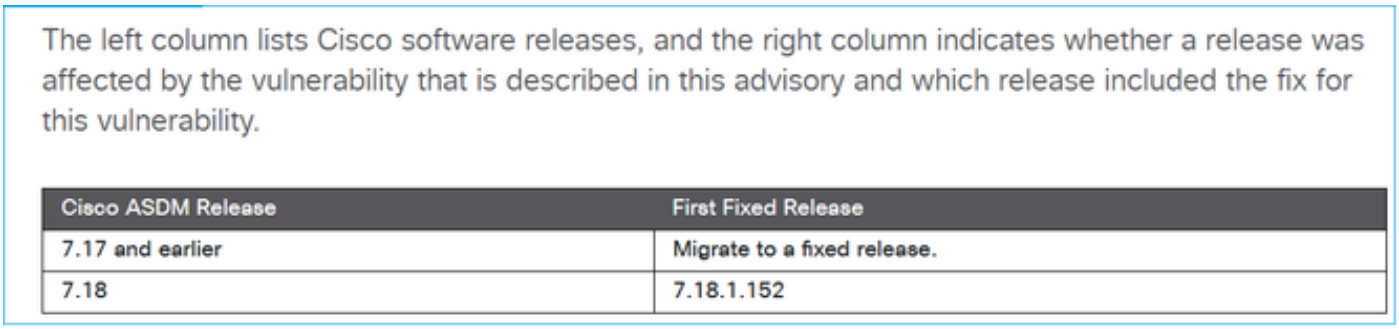
2단계: Cisco Security Advisories and Cisco Bug Search 툴에서 CVE를 검색합니다.

권고 사항 페이지로 이동합니다.

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



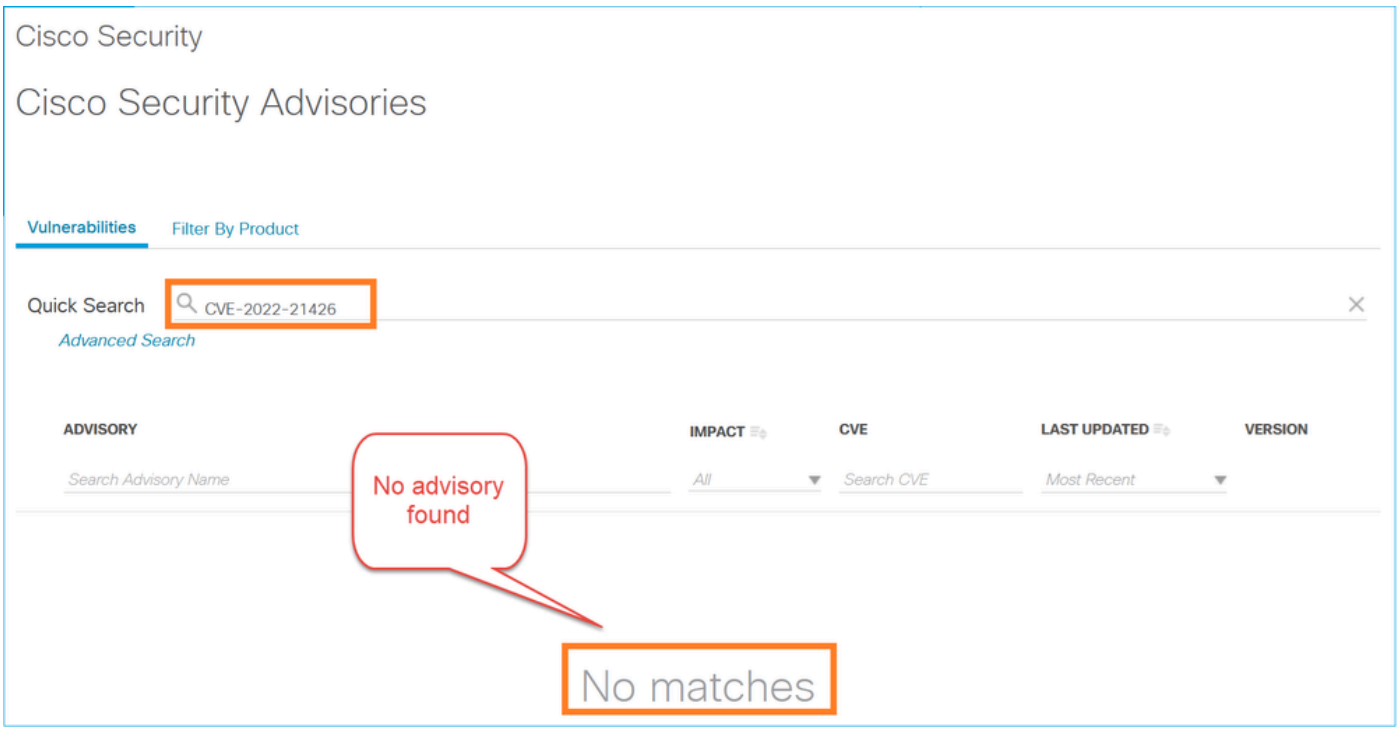
권고 사항을 열고 ASDM이 영향을 받는지 확인합니다. 예를 들면 다음과 같습니다.

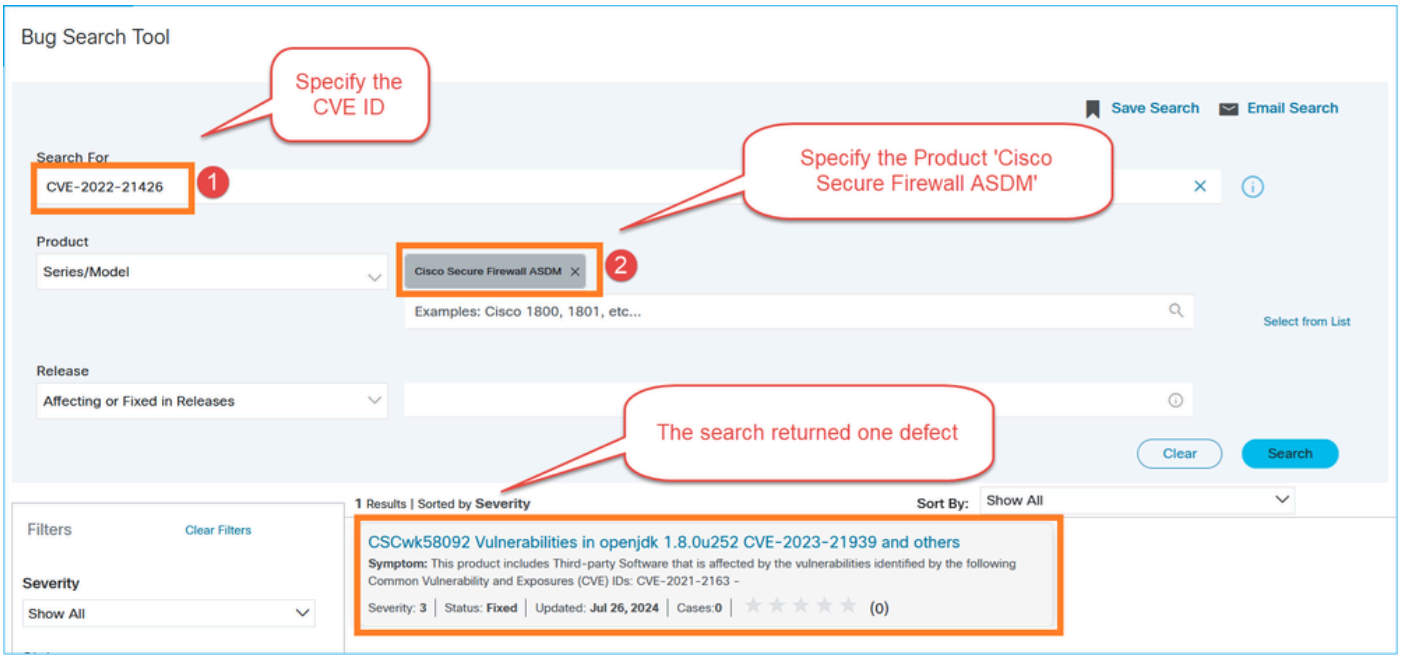


The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

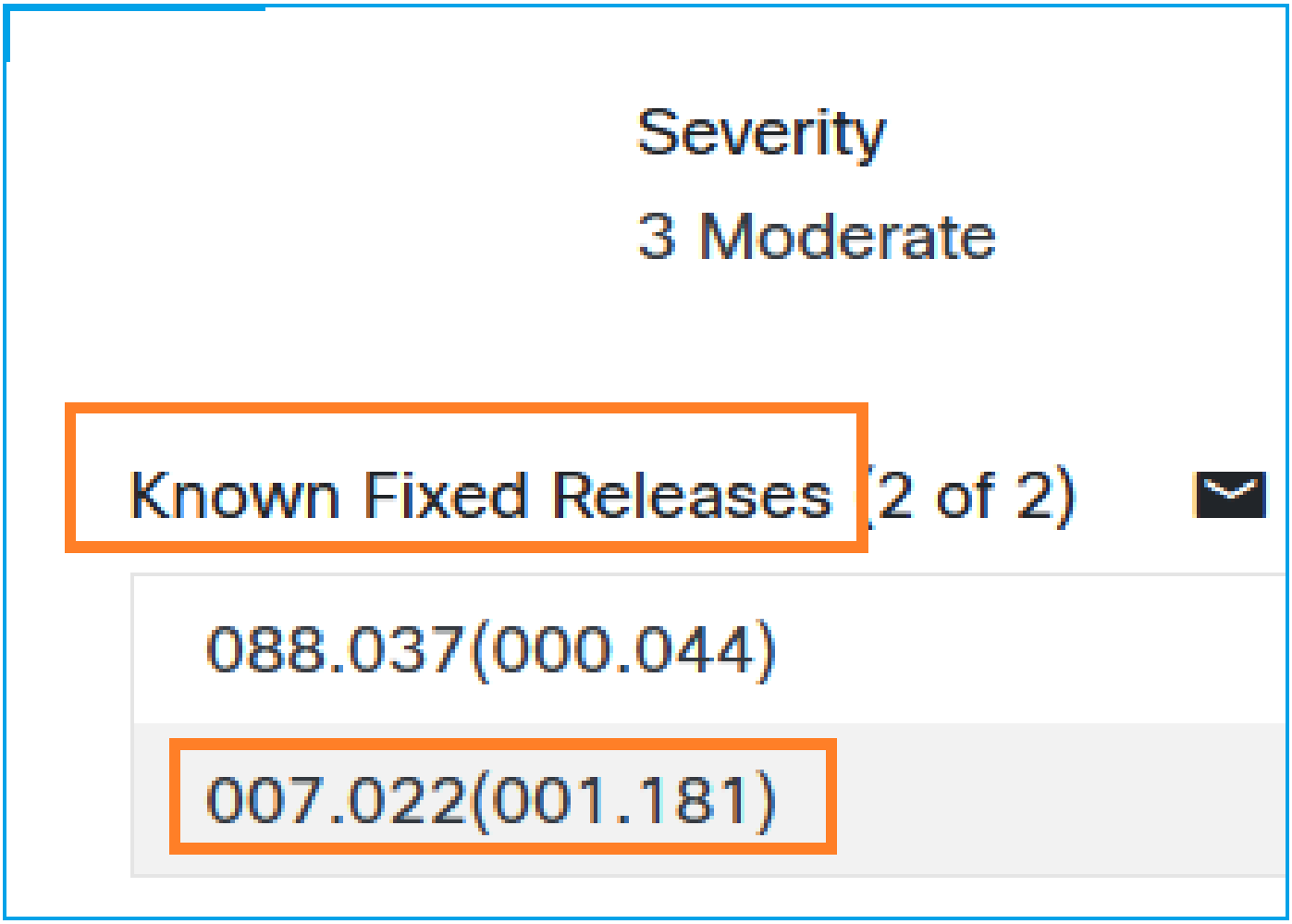
Cisco ASDM Release	First Fixed Release
7.17 and earlier	Migrate to a fixed release.
7.18	7.18.1.152

권고 사항이 없는 경우 Cisco Bug Search Tool(Cisco 버그 검색 툴)에서 CVE ID를 검색하십시오 (https://bst.cisco.com/bugsearch)





이 경우 결함이 확인되었습니다. 클릭하여 해당 세부사항과 'Known Fixed Releases' 섹션을 확인합니다.



7.22.1.181 ASDM 소프트웨어 릴리스에서 결함이 수정되었습니다.

지정된 CVE ID에 대한 권고 툴 및 버그 검색 툴의 검색에서 아무 것도 반환되지 않을 경우 Cisco

TAC와 협력하여 ASDM이 CVE의 영향을 받는지 확인해야 합니다.

참조

- ASDM 컨피그레이션 가이드
- 모델당 Cisco ASA 및 ASDM 호환성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.