Troubleshoot ASDM TLS Security, Certificate and Vulnerability Problems

Contents

Introduction

This document describes the troubleshooting process for ASDM Transport Layer Security (TLS) security, certificate and vulnerability problems.

Background

The document is part of the Adaptive Security Appliance Device Manager (ASDM) troubleshoot series along with these documents:

- Troubleshoot ASDM Launch Problems
- Troubleshoot ASDM Configuration, Authentication and Other Problems
- Troubleshoot ASDM License, Upgrade and Compatibility Problems

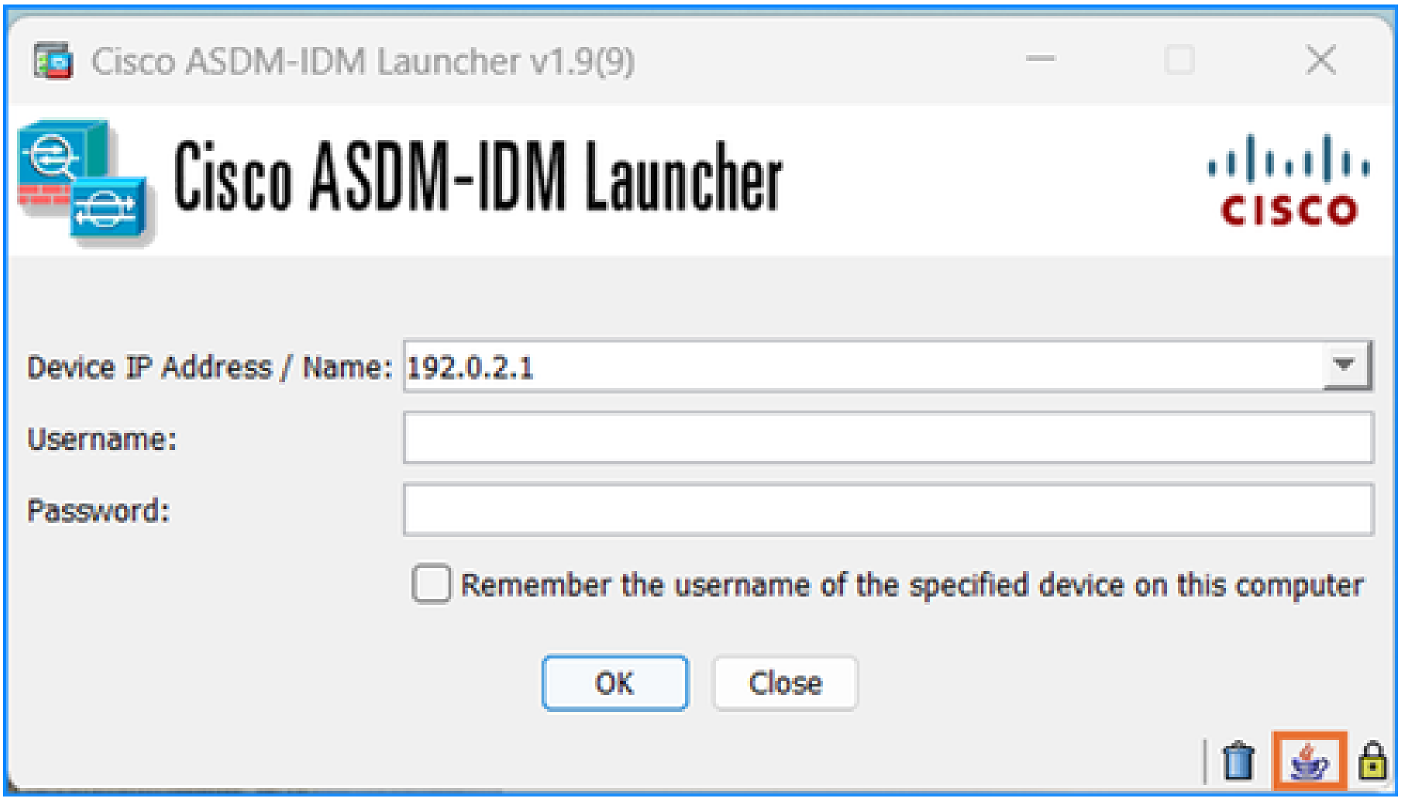
ASDM TLS Cipher Problems

Problem 1. ASDM cannot connect to the firewall due to TLS cipher problems

ASDM cannot connect to the firewall. One or more of the these symptoms are observed:

- ASDM shows the "Could not open device" or the "**Unable to launch device manager from <ip>**" error messages.

- The output of the **show ssl error** command contains the “**SSL lib error. Function: ssl3_get_client_hello Reason: no shared cipher**” message.
- The Java console logs show the “**javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure**” error message:


Cisco ASDM-IDM Launcher v1.9(9)
Cisco ASDM-IDM Launcher
CISCO
Device IP Address / Name: 192.0.2.1
Username:
Password:
□ Remember the username of the specified device on this computer
OK
Close

<#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)
```

Troubleshoot – Recommended Actions

A common root cause of the symptoms is the TLS cipher suite negotiation failure between the ASDM and ASA. In these cases, depending on the cipher configuration, the user needs to adjust the certificate on the ASMD and/or ASA side.

Go through one or more of these steps until the connectivity is successful:

1. In the case of ASDM with OpenJRE if strong TLS cipher suites are used, apply the workaround from the software Cisco bug ID CSCvv12542 “ASDM open JRE should use higher ciphers by default”:
2. Start Notepad (run as an administrator)
3. Open the file: **C:\Program Files\Cisco Systems\ASDM\jre\lib\security\java.security**
4. Search for: crypto.policy=unlimited

5. Remove # in front of that line so that all encryption options are available
6. Save

2. Change the TLS cipher suites on the 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
```

The cipher options for TLSv1.2:

<#root>

```
ASA(config)#
```

`ssl cipher tlsv1.2 ?`

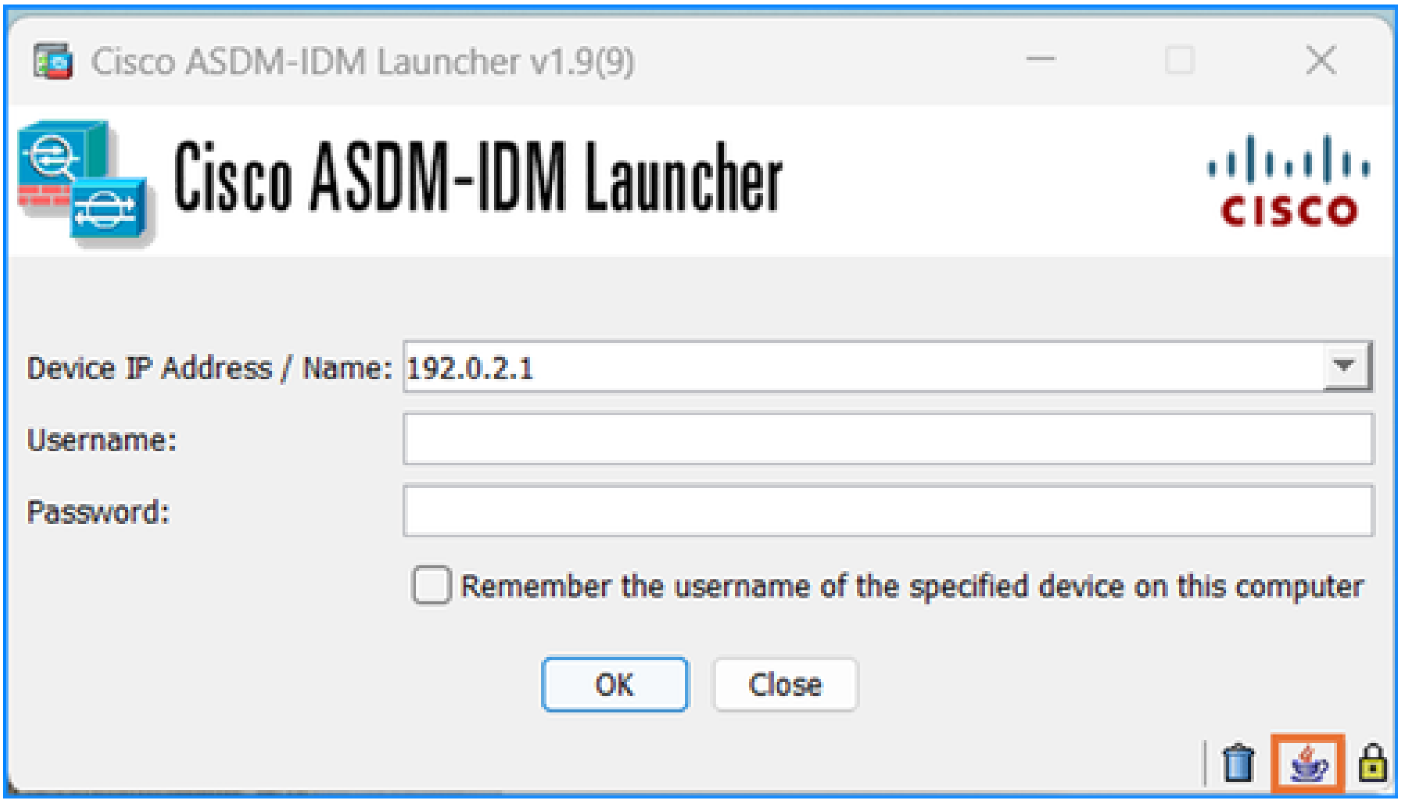
```
configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration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

Warning: The changes in the **ssl cipher** command are applied to the entire firewall, including the site to site or remote access VPN connections.

Problem 2. ASDM cannot connect to due to TLS1.3 handshake failure

The ASDM cannot connect to due to TLS1.3 handshake failure.

The Java console logs show the “**java.lang.IllegalArgumentException: TLSv1.3**” error message:



Cisco ASDM-IDM Launcher v1.9(9)

Device IP Address / Name: 192.0.2.1

Username:

Password:

☐ Remember the username of the specified device on this computer

<#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)
```

Troubleshoot – Recommended Actions

TLS 1.3 version must be supported on both ASA and ASDM. TLS version 1.3 is supported in ASA versions 9.19.1 and later (Release Notes for the Cisco Secure Firewall ASA Series, 9.19(x)). The Oracle Java version 8u261 or later is required to support TLS version 1.3 (Release Notes for Cisco Secure Firewall ASDM, 7.19(x)).

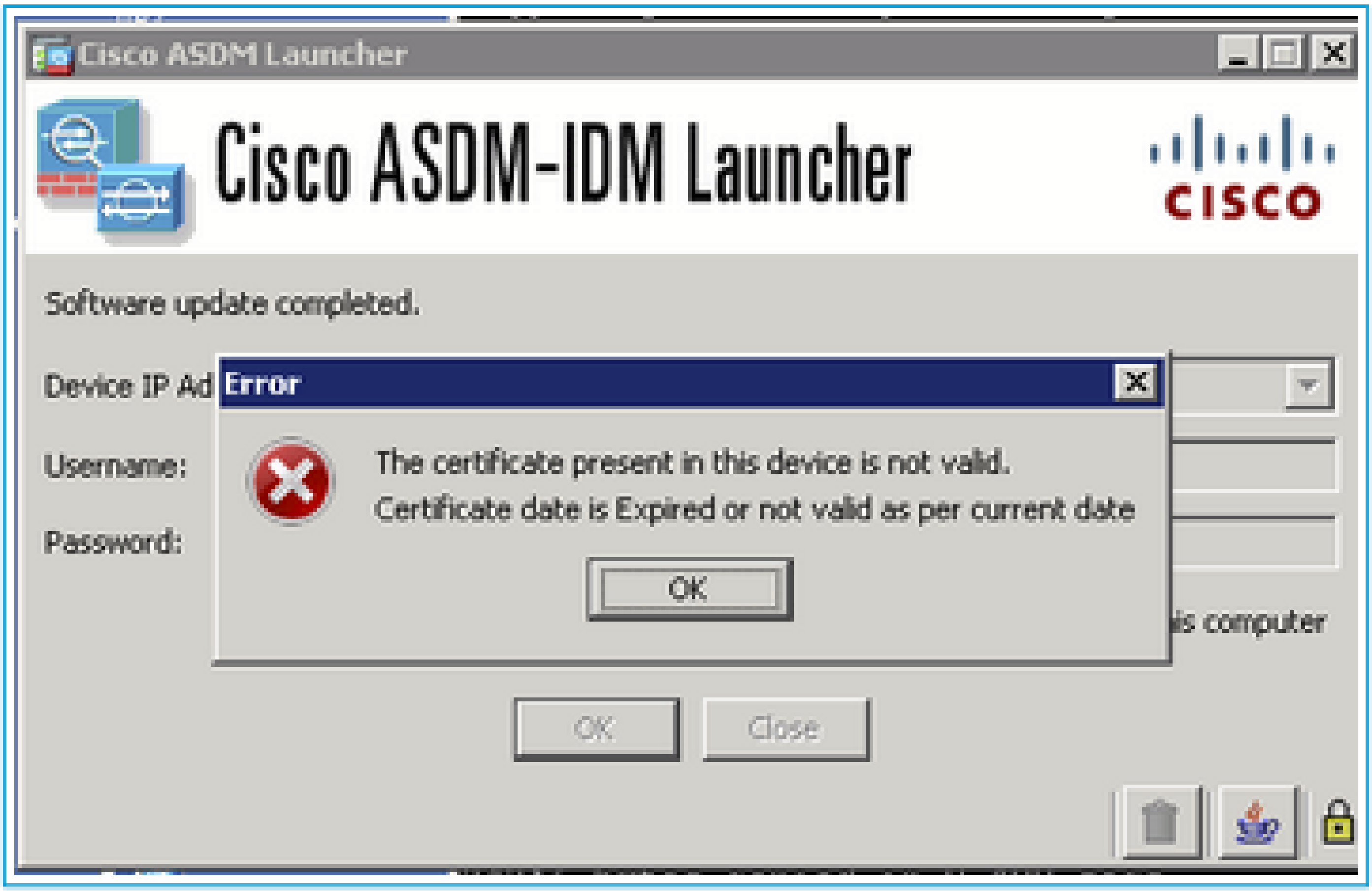
References

1. Release Notes for the Cisco Secure Firewall ASA Series, 9.19(x)
2. Release Notes for Cisco Secure Firewall ASDM, 7.19(x)

ASDM Certificate Problems

Problem 1. “The certificate present in this device is not valid. The certificate date is expired or not valid as a per current dates.” error message

The error message is shown when running ASDM: "The certificate present in this device is not valid. The certificate date is expired or not valid as a per current dates."



The certificate present in this device is not valid.
Certificate date is Expired or not valid as per current date

OK

Similar symptoms are described in the release notes:

“ASDM's self-signed certificate not valid due to a time and date mismatch with ASA—ASDM validates the self-signed SSL certificate, and if the ASA's date is not within the certificate's Issued On and Expires On date, ASDM will not launch. See ASDM Compatibility Notes

Troubleshoot – Recommended Actions

1. Check and confirm expired certificates:

<#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. In the ASA Command Line Interface (CLI), remove the line **ssl trust-point <cert> <interface>**, where the **<interface>** is the nameif used for ASDM connections. The ASA uses self-signed certificate for ASDM connections.
2. If there is no self-signed certificate, generate one. In this example, the **SELF-SIGNED** name is used as a true point name:

<#root>

```
conf t



crypto ca trustpoint SELF-SIGNED



enrollment self



fqdn <fqdn>



subject-name CN=<cn>,O=<org>,C=<country>,St=<state>,L=<location>
```

```
exit

crypto ca enroll SELF-SIGNED

crypto ca enroll SELF-SIGNED

WARNING: The certificate enrollment is configured with an <fqdn>

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. Associate the generated certificate with the interface:

<#root>

```
ssl trust-point SELF-SIGNED <interface>
```

4. Verify the certificate:

<#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. Verify the certificate association with the interface:

```
<#root>

#

 show run all ssl
```

Problem 2. How to install or renew certificates using the ASDM or ASA CLI?

The users want to clarify the steps to install or renew certificates using the ASDM or ASA CLI.

Recommended Actions

Refer to the guides to install and renew certificates:

- ASA: SSL Digital Certificate Installation and Renewal
- Install and Renew Certificates on ASA Managed by CLI

ASDM Vulnerability Problems

This section covers the most common ASDM Vulnerability-related problems.

Problem 1. Vulnerability detected on ASDM

In case you detect a vulnerability on ASDM.

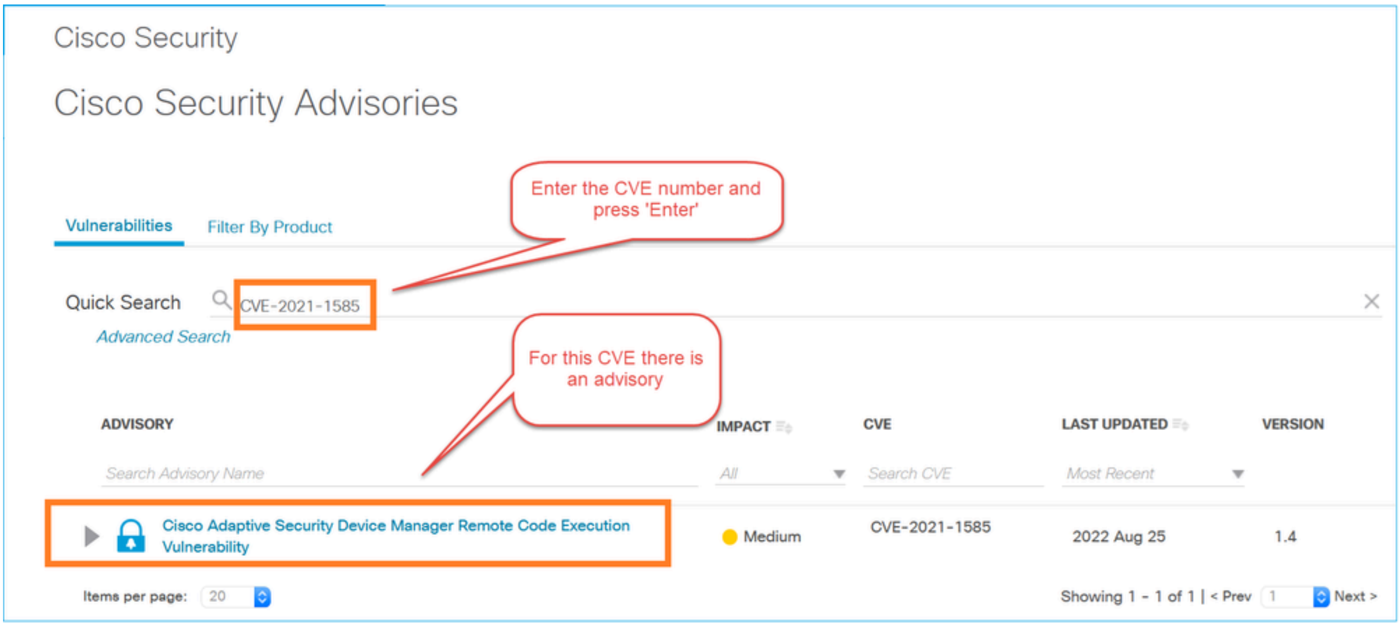
Troubleshoot – Recommended Steps

Step 1: Identify the CVE ID (for example, CVE-2023-21930)

Step 2: Search for the CVE in the Cisco Security Advisories and Cisco Bug Search tool:

Navigate to the advisory page:

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



Cisco Security

Cisco Security Advisories

Enter the CVE number and press 'Enter'

Quick Search: CVE-2021-1585

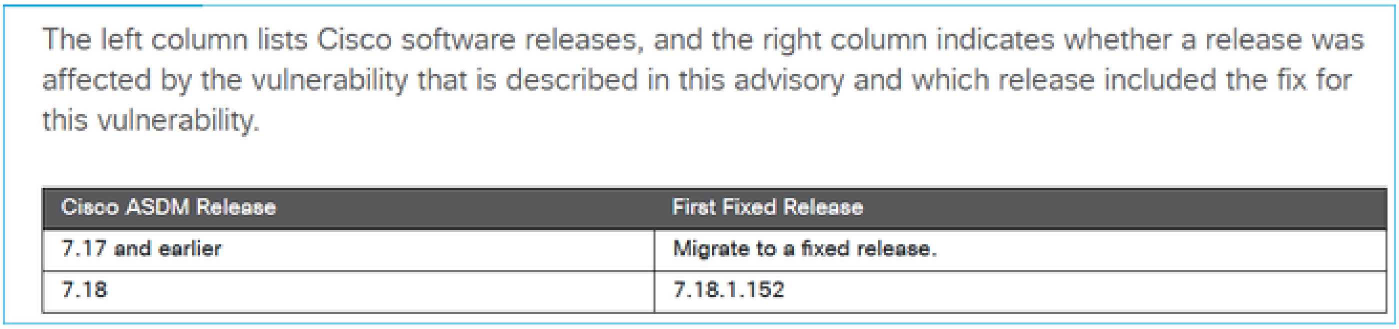
For this CVE there is an advisory

ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
Cisco Adaptive Security Device Manager Remote Code Execution Vulnerability	Medium	CVE-2021-1585	2022 Aug 25	1.4

Items per page: 20

Showing 1 - 1 of 1

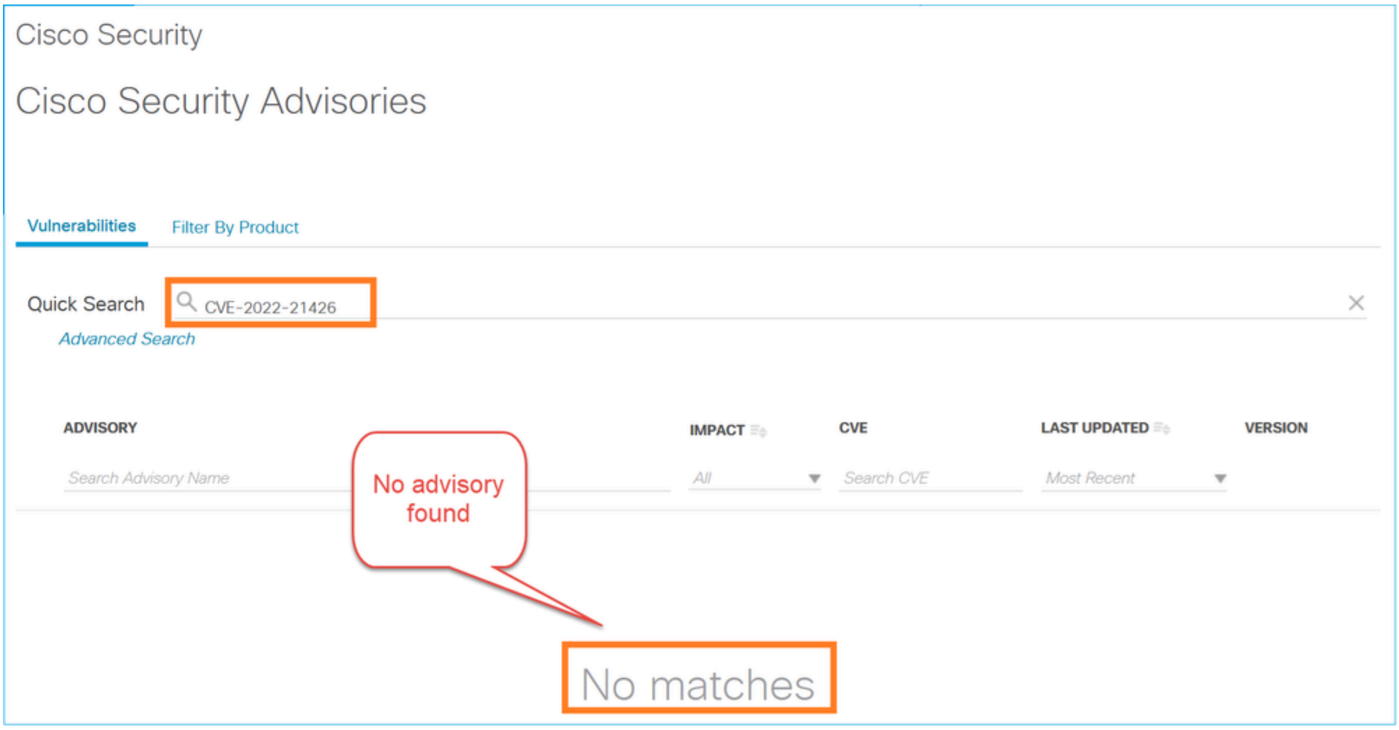
Open the advisory and check if ASDM is affected, for example:



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

In case there is no advisory found, search for the CVE ID in the Cisco Bug Search Tool (https://bst.cisco.com/bugsearch)



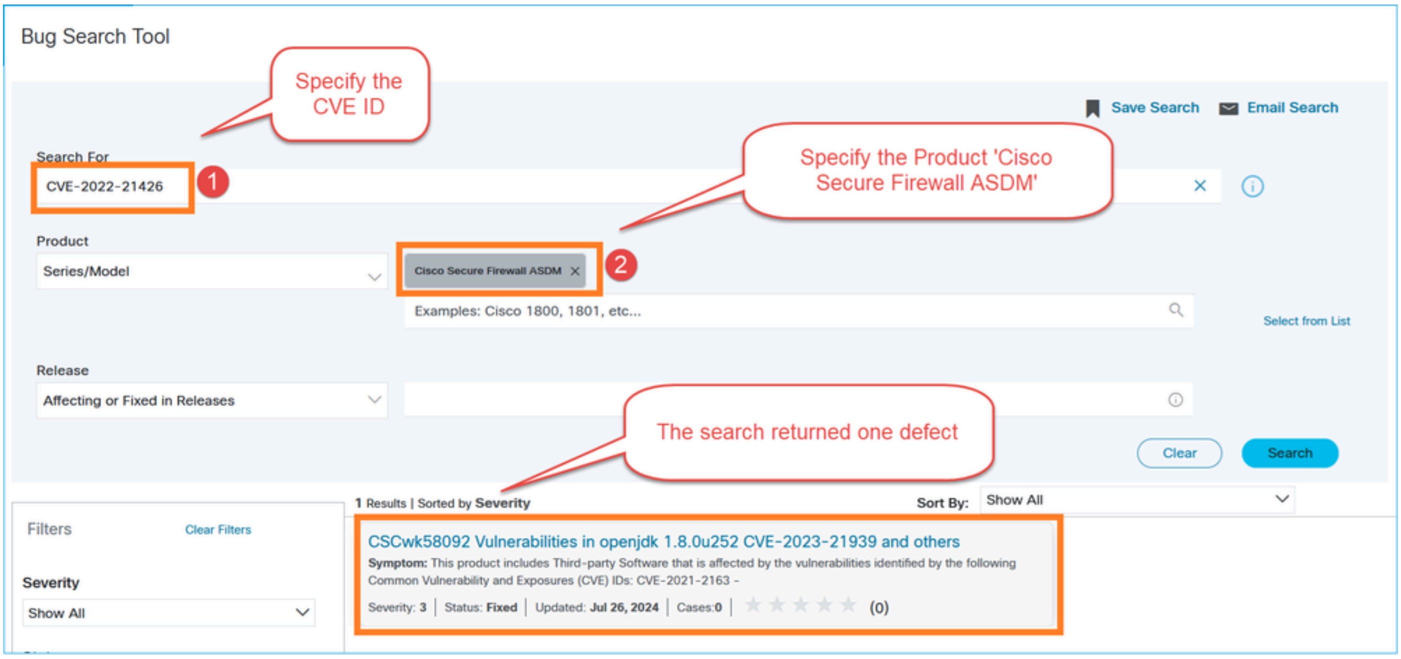
Cisco Security

Cisco Security Advisories

Quick Search: CVE-2022-21426

No advisory found

No matches



Bug Search Tool

Specify the CVE ID

Search For: CVE-2022-21426 (1)

Specify the Product 'Cisco Secure Firewall ASDM'

Product: Series/Model — Cisco Secure Firewall ASDM (2)

Release: Affecting or Fixed in Releases

The search returned one defect

1 Results | Sorted by **Severity**

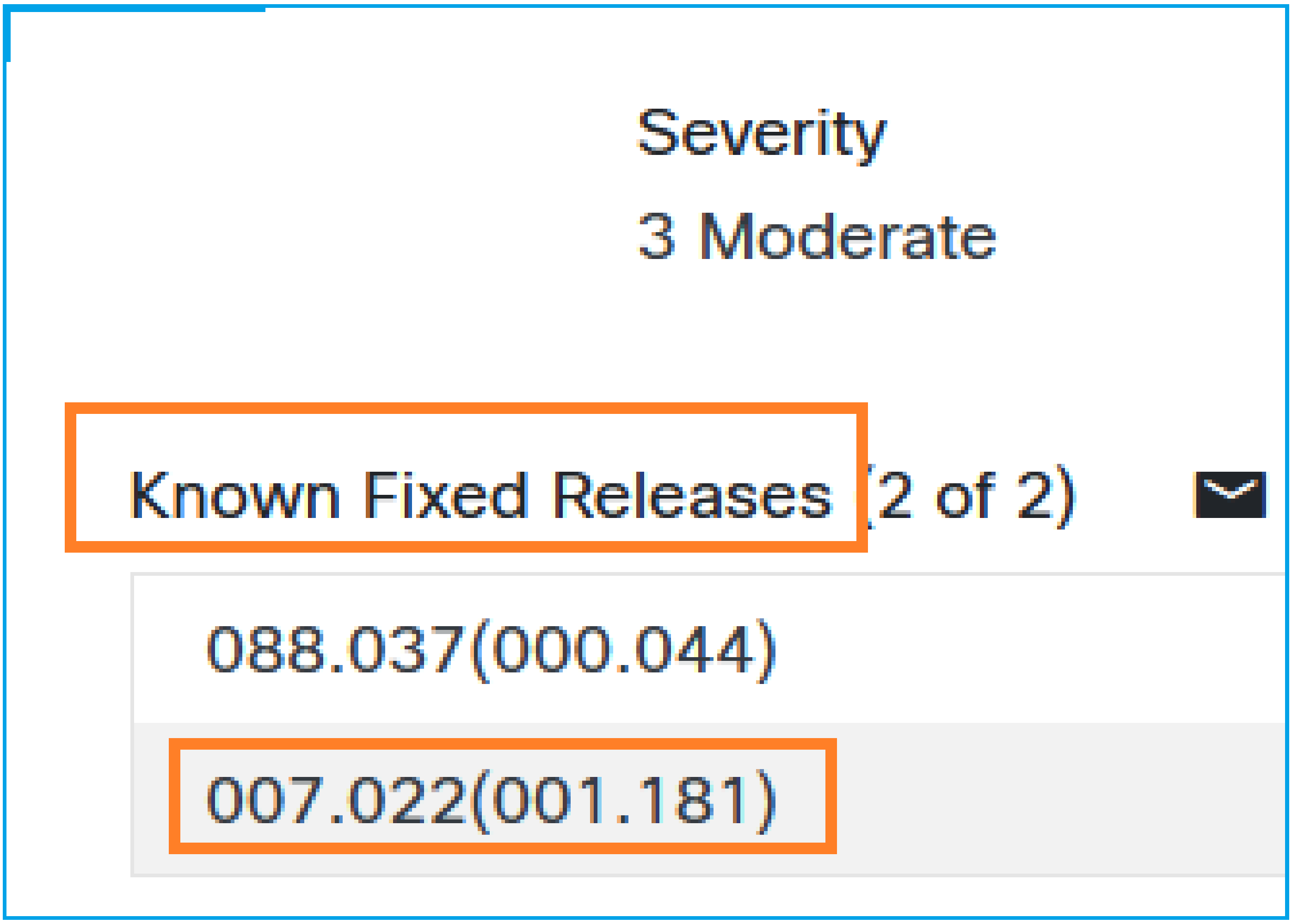
Sort By: Show All

CSCwk58092 Vulnerabilities in openjdk 1.8.0u252 CVE-2023-21939 and others

Symptom: This product includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2021-2163 -

Severity: **3** | Status: **Fixed** | Updated: **Jul 26, 2024** | Cases:**0** | ☆☆☆☆☆ (0)

In this case a defect was identified. Click on it and check its details and the ‘Known Fixed Releases’ section:



Severity

3 Moderate

Known Fixed Releases (2 of 2)

088.037(000.044)

007.022(001.181)

The defect is fixed in 7.22.1.181 ASDM software release.

If the searches in the advisory tool and bug search tool for the specified CVE ID didn’t return anything, you need to work with Cisco TAC to clarify if ASDM is affected by the CVE.

References

- ASDM Configuration Guides
- Cisco ASA and ASDM Compatibility per Model