CiscoFirepower脅威対策ソフトウェアのSnort 3検出エンジンにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-ftd-snort3-uAnUntcV
初公開日 : 2023-11-01 16:00
バージョン 1.0 : Final
CVSSスコア : 4.0
回避策 : Yes
Cisco バグ ID : CSCwc59953

CVE-2023-20070

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

CiscoFirepower脅威対策(FTD)ソフトウェアのTLS 1.3の実装における脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンを予期せず再起動させる可能性があります。

この脆弱性は、TLS 1.3セッション中のメモリ割り当ての処理方法における論理エラーに起因します。特定の時間ベースの制約の下で、攻撃者は該当デバイスを介して巧妙に細工されたTLS 1.3メッセージシーケンスを送信することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はSnort 3検出エンジンのリロードを引き起こし、その結果サービス妨害(DoS)状態が発生する可能性があります。Snort検出エンジンのリロード中に、FTDデバイスを通過し、Snort検出エンジンに送信されるパケットはドロップされます。Snort検出エンジンが自動的に再起動します。手動による介入は必要ありません。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。本脆弱性に対処する回避策がいくつかあります。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort3-uAnUntcV

このアドバイザリは、Cisco ASA、FTD、およびFMCセキュリティアドバイザリバンドル公開の2023年11月版リリースの一部です。アドバイザリの完全なリストとそのリンクについては、『Cisco Event Response: November 2023 Semiannual Cisco ASA, FMC, and FTD Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

公開時点では、この脆弱性はCisco FTDソフトウェアの脆弱性が存在するリリースを実行しているデバイスに影響を与え、次の条件の両方に該当していました。

- デバイスはSnort 3を実行していました。
- デバイスは、TLS 1.3復号化が有効なSSLポリシーを使用していました。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

Cisco FTDソフトウェアのSnort設定の確認

Snort 3がCisco FTDソフトウェアで実行されているかどうかを確認するには、「Firepower脅威対策(FTD)で実行されているアクティブなSnortのバージョンの判別」を参照してください。この脆弱性を不正利用するには、Snort 3をアクティブにする必要があります。

Cisco FTDソフトウェアのSSLポリシー設定の確認

SSL復号化ポリシーはデフォルトでは設定されていません。

FTDソフトウェアCLIを使用したCisco FTDソフトウェアSSLポリシー設定の確認

Cisco FTDソフトウェアを実行しているデバイスにSSLポリシーが設定されているかどうかを確認するには、Cisco FTDソフトウェアのCLIにログインし、show ssl-policy-configコマンドを使用します。

コマンドの出力に「SSL policy not yet applied」と表示されている場合、次の例に示すように、デバイスはこの脆弱性の影響を受けません。

```
<#root>

>

show ssl-policy-config


SSL policy not yet applied
```

コマンド出力にポリシーが示されている場合、デバイスにはSSLポリシーが適用されており、TLS 1.3復号化が有効になっている場合、次の例に示すように、この脆弱性の影響を受ける可能性があります。

```
<#root>
```

```
>
show ssl-policy-config


==================[ CSCwc59953 ]==================
================[ Default Action ]================
Default Action             : Do Not Decrypt
...
```

CiscoFirepowerデバイスマネージャソフトウェアで管理されているデバイスのCisco FTDソフトウェアSSLポリシー設定の確認

CiscoFirepowerデバイスマネージャ(FDM)ソフトウェアで管理されているデバイスにSSLポリシーが設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco FTDソフトウェアのWebインターフェイスにログインします。
2. メインメニューから [ポリシー（Policies）] を選択します。
3. SSL Decryptionタブを選択します。
    - SSL復号化が有効になっていない場合、デバイスはこの脆弱性の影響を受けません。
    - ポリシー名がリストされている場合、TLS 1.3復号化が有効になっていれば、デバイスはこの脆弱性の影響を受ける可能性があります。

SSL復号化ポリシーの詳細については、『Firepower Device Manager用CiscoFirepower脅威対策コンフィギュレーションガイド』の「SSL復号化」の章を参照してください。

Cisco Software Management Centerソフトウェアによって管理されるデバイスのCisco FTDFirepowerSSLポリシー設定の確認

SSLポリシーが、Cisco Network Management Center(FMC)ソフトウェアによって管理されるFirepowerに設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco FMCソフトウェアWebインターフェイスにログインします。
2. [ポリシー（Policies）] メニューから [アクセス制御（Access Control）] を選択します。
3. 適切なアクセスコントロールポリシーを選択します。
4. [編集（Edit）] アイコン（鉛筆の形）をクリックします。
5. SSL Policy領域を確認します。
    - Noneがリストされている場合、そのデバイスはこの脆弱性の影響を受けません。
    - Policy Nameがリストされている場合、TLS 1.3 Decryptionが有効になっていると、デバイスはこの脆弱性の影響を受ける可能性があります。

SSL復号化ポリシーの詳細については、『Cisco Secure Firewall Management Centerコンフィギュレーションガイド』の「SSLポリシー」の章を参照してください。

Cisco Defense Orchestratorによって管理されるデバイスのCisco FTDソフトウェアSSLポリシ

ー設定の確認

Cisco Defense Orchestratorで管理されているデバイスにSSLポリシーが設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco Defense Orchestrator Web インターフェイスにログインします。
2. Cisco Defense OrchestratorのPoliciesメニューから、FTD Policiesを選択します。
3. FTDのPoliciesメニューから、Access Controlを選択します。
4. 適切なアクセスコントロールポリシーを選択します。
5. [編集（Edit）] アイコン（鉛筆の形）をクリックします。
6. Decryption Policy領域を調べます。
    - Noneがリストされている場合、そのデバイスはこの脆弱性の影響を受けません。
    - Policy Nameがリストされている場合、TLS 1.3 Decryptionが有効になっていると、デバイスはこの脆弱性の影響を受ける可能性があります。

Cisco Defense Orchestrator管理対象デバイスの詳細については、Cisco Defense Orchestratorのドキュメントを参照してください。

Cisco Defense Orchestratorで管理されているCisco FMCデバイスのSSL復号化ポリシーの詳細については、『Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator』の「復号化ポリシー」の章を参照してください。

Cisco Defense Orchestratorで管理されるCisco FDMデバイスのSSL復号化ポリシーの詳細については、『Cisco Defense OrchestratorでのFDMデバイスの管理』ガイドの「SSL復号化ポリシー」セクションを参照してください。

Cisco FTDソフトウェアのTLS 1.3復号化設定の確認

TLS 1.3復号化のデフォルト設定は、SSLポリシーを設定するときのプラットフォームによって異なります。Cisco FDM制御デバイスのTLS 1.3復号化は、Cisco FTDリリース7.3.0まで提供されないことに注意してください。TLS 1.3の復号化は、Cisco FMCおよびCisco Defense Orchestratorによって管理されるデバイス用のCisco FTDリリース7.2.0で提供されます。

プラットフォームのデフォルト設定は次のとおりです。

- TLS 1.3復号化は、Cisco FDMソフトウェアによって管理されるデバイスではデフォルトで有効になっていません。
- Cisco FMCソフトウェアで管理されているデバイスでは、TLS 1.3復号化はデフォルトで有効になっていません。
- Cisco Discovery Orchestratorソフトウェアによって管理されるデバイスでは、TLS 1.3の復号化がデフォルトで有効になっています。

FTDソフトウェアCLIを使用したCisco FTDソフトウェアTLS 1.3復号化設定の確認

CLIでデバイスにTLS 1.3復号化が設定されているかどうかを確認するには、Cisco FTDソフトウェアCLIにログインし、grep tls13 /ngfw/var/sf/detection_engines/*/ssl/ssl.rulesコマンドを使用します。

- コマンドの出力に「tls13_decryption」「false」が表示された場合、そのデバイスはこの脆弱性の影響を受けません。
- コマンドの出力に何も表示されない場合、デバイスはこの脆弱性の影響を受けません。
- コマンドの出力に「tls13_decryption」「true」と表示される場合、デバイスにSSLポリシーが適用されており、TLS 1.3の復号化が有効になっている場合にこの脆弱性の影響を受ける可能性があります。次に例を示します。

```
<#root>

>

expert


admin@ftd:~$
admin@ftd:~$

grep tls13 /ngfw/var/sf/detection_engines/*/ssl/ssl.rules


  "tls13_decryption" "true";
```

Cisco FDMソフトウェアで管理されるデバイスのCisco FTDソフトウェアTLS 1.3復号化設定の確認

Cisco FDMソフトウェアによって管理されているデバイスでTLS 1.3復号化が設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco FTDソフトウェアのWebインターフェイスにログインします。
2. メインメニューから [ポリシー（Policies）] を選択します。
3. SSL Decryptionタブを選択します。
4. SSL Decryption Settingsボタンをクリックします。
5. [詳細] タブをクリックします。
    - TLS 1.3 Decryptionスライダが有効になっていない場合、そのデバイスはこの脆弱性の影響を受けません。
    - TLS 1.3 TLS 1.3 Decryptionスライダが有効になっている場合、デバイスはこの脆弱性の影響を受けます。

TLS 1.3の復号化の詳細については、『Firepower Device Manager用CiscoFirepower脅威対策コンフィギュレーションガイド』の「高度なトラフィックおよび復号化できないトラフィックの設定」セクションを参照してください。

Cisco FMCソフトウェアによって管理されるデバイスのCisco FTDソフトウェアTLS 1.3復号化設定の確認

Cisco FMCソフトウェアで管理されているデバイスでTLS 1.3復号化が設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco FMCソフトウェアWebインターフェイスにログインします。
2. Policiesメニューから、SSLを選択します。
3. 適切なSSLポリシーを選択します。
4. [編集（Edit）] アイコン（鉛筆の形）をクリックします。
5. Advanced Settingsタブをクリックします。
    - Enable TLS 1.3 Decryptionボックスにチェックマークが入っていない場合、そのデバイスはこの脆弱性の影響を受けません。
    - Enable TLS 1.3 Decryptionボックスにチェックマークが入っている場合、そのデバイスはこの脆弱性の影響を受けます。

TLS 1.3の復号化の詳細については、『Cisco Secure Firewall Management Centerコンフィギュレーションガイド』の「SSLポリシーの詳細オプション」セクションを参照してください。

Cisco Defense Orchestratorソフトウェアで管理されるデバイスのCisco FTDソフトウェアTLS 1.3復号化設定の確認

Cisco Defense Orchestratorで管理されているデバイスでTLS 1.3復号化が設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco Defense Orchestrator Web インターフェイスにログインします。
2. Cisco Defense OrchestratorのPoliciesメニューから、FTD Policiesを選択します。
3. FTDのPoliciesメニューから、Decryptionを選択します。
4. 適切な復号化ポリシーを選択します。
5. [編集（Edit）] アイコン（鉛筆の形）をクリックします。
6. Advanced Settingsタブをクリックします。
    - Enable TLS 1.3 Decryptionが有効になっていない場合、そのデバイスはこの脆弱性の影響を受けません。
    - Enable TLS 1.3 Decryptionが有効になっている場合、デバイスはこの脆弱性の影響を受けます。

Cisco Defense Orchestratorによって管理されるデバイスの詳細については、Cisco Defense Orchestratorのマニュアルを参照してください。

TLS 1.3の復号化の詳細については、『Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator』の「Decryption Policy Advanced Options」セクションを参照してください。

Cisco Defense Orchestratorで管理されているCisco FDMデバイスのTLS 1.3復号化の詳細につ

いては、『Cisco Defense OrchestratorでのFDMデバイスの管理』の「SSL復号化ポリシー」セクションを参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下の製品には影響を与えないことを確認しました。

- Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア
- Cisco FMC ソフトウェア
- オープンソースSnort 2
- オープンソースSnort 3

回避策

この脆弱性に対処する回避策と緩和策があります。この脆弱性に対する攻撃ベクトルを排除するには、次の2つのオプションのいずれかを使用できます。2つのオプションのうち1つだけを適用する必要があります。

- Snort 2に戻す
- TLS 1.3復号化の無効化

Snort 2への復帰

ダウングレードする前に、『Firepower Device Manager用CiscoFirepower脅威対策コンフィギュレーションガイド』の「Snort 2とSnort 3の間の切り替え」セクションにある「はじめに」セクションを参照してください。

注：Snort 2にダウングレードすると、アクティブな認証で顧客ポリシー、NAPのカスタマイズ、およびホスト名のリダイレクトが削除されます。復帰が展開に与える影響については、Technical Assistance Center(TAC)にお問い合わせください。

FDMソフトウェアで管理されているCisco FTDデバイスのSnort 2への復帰

Cisco FDMソフトウェアで管理されているデバイスでSnort 2に戻すには、次の手順を実行します。

1. Cisco FTDソフトウェアのWebインターフェイスにログインします。
2. メインメニューから、Deviceを選択します。
3. Updates領域で、View Configurationを選択します。
4. Intrusion Ruleセクションで、Downgrade to 2.0を選択します。

上記の変更を行った後、Cisco FTDデバイスに変更を導入します。

Snort 2への復帰の詳細については、『Firepower Device Manager用CiscoFirepower脅威対策設定ガイド』の「Snort 2とSnort 3の切り替え」セクションを参照してください。

FMCソフトウェアで管理されているCisco FTDデバイスのSnort 2への復帰

Cisco FMCソフトウェアで管理されているデバイスでSnort 2に戻すには、次の手順を実行します。

1. Cisco FMCソフトウェアWebインターフェイスにログインします。
2. [デバイス（Devices）] メニューから [デバイス管理（Device Management）] を選択します。
3. 適切なCisco FTDデバイスを選択します。
4. [編集（Edit）] アイコン（鉛筆の形）をクリックします。
5. Deviceタブを選択します。
6. Inspection Engine領域で、Revert to Snort 2を選択します。

上記の変更を行った後、FTDデバイスに変更を展開します。

Snort 2への復帰の詳細については、『Cisco Secure Firewall Management Center Snort 3コンフィギュレーションガイド』の「Snort 3インスペクションエンジン」の章を参照してください。

Cisco Defense Orchestratorで管理されているCisco FTDデバイスのSnort 2への復帰

Cisco Defense Orchestratorによって管理されているデバイスでSnort 2に戻すには、次の手順を実行します。

1. Cisco Defense Orchestrator Web インターフェイスにログインします。
2. ナビゲーションバーでInventoryをクリックします。
3. Devicesタブをクリックします。
4. FTDタブをクリックし、元に戻すデバイスをクリックします。
5. 右側にあるDevice Actionsペインで、Upgradeをクリックします。
6. アップグレードの切り替えを侵入防御エンジンに設定します。
7. Revert to Snort Engine 2.0をクリックします。

上記の変更を行った後、Cisco FTDデバイスに変更を導入します。

Cisco Defense Orchestrator管理対象デバイスの詳細については、Cisco Defense Orchestratorのドキュメントを参照してください。

Cisco Defense Orchestratorで管理されているCisco FMCデバイスをSnort 2に戻す方法の詳細については、『Cisco Secure Firewall Management Center Snort 3コンフィギュレーションガイド』の「Snort 3インスペクションエンジン」の章を参照してください。

Cisco Defense Orchestratorで管理されているCisco FDMデバイスをSnort 2に戻す方法の詳細については、『Cisco Defense OrchestratorでFDMデバイスを管理するガイド』の「FDM管理対象デ

バイスのSnort 3.0から戻す」セクションを参照してください。

TLS 1.3復号化の無効化

この緩和策は、クライアントとサーバの接続に影響を与える可能性があります。TLS 1.3の復号化が無効になっている場合、TLS接続は復号化ルールに一致しながらTLS 1.2にダウングレードされます。導入への影響は、Cisco FTDデバイス経由で接続するクライアントとサーバによって異なります。これが導入に及ぼす影響については、Technical Assistance Center(TAC)にお問い合わせください。

FDMソフトウェアで管理されているCisco FTDソフトウェアデバイスのTLS 1.3を無効にする

Cisco FDMソフトウェアによって管理されているデバイスでTLS 1.3復号化を無効にするには、次の手順を実行します。

1. Cisco FTDソフトウェアのWebインターフェイスにログインします。
2. メインメニューから [ポリシー（Policies）] を選択します。
3. SSL Decryptionタブを選択します。
4. SSL Decryption Settingsボタンをクリックします。
5. [詳細] タブをクリックします。
6. TLS 1.3 Decryption設定を無効にします。
7. [OK] をクリックします。

上記のポリシーを変更した後、新しいポリシーをCisco FTDデバイスに導入します。

TLS 1.3の復号化の詳細については、『Firepower Device Manager用のCiscoFirepower脅威対策コンフィギュレーションガイド』の「高度なトラフィックおよび復号化不能なトラフィックの設定」セクションを参照してください。

FMCソフトウェアで管理されているCisco FTDソフトウェアデバイスのTLS 1.3を無効にする

Cisco FMCソフトウェアで管理されているデバイスでTLS 1.3復号化を無効にするには、次の手順を実行します。

1. Cisco FMCソフトウェアWebインターフェイスにログインします。
2. Policiesメニューから、SSLを選択します。
3. 適切なSSLポリシーを選択します。
4. [編集（Edit）] アイコン（鉛筆の形）をクリックします。
5. Advanced Settingsタブをクリックします。
6. Enable TLS 1.3 Decryptionボックスのチェックマークを外します。
7. Saveをクリックして変更を保存します。

上記のポリシーを変更した後、新しいポリシーをFTDデバイスに展開します。

TLS 1.3の復号化の詳細については、『Cisco Secure Firewall Management Centerコンフィギュレ

ーションガイド』の「SSLポリシーの詳細オプション」セクションを参照してください。

Cisco Defense Orchestratorで管理されるCisco FTDソフトウェアデバイスのTLS 1.3を無効にする

Cisco Defense Orchestratorで管理されているデバイスでTLS 1.3復号化を無効にするには、次の手順を実行します。

1. Cisco Defense Orchestrator Web インターフェイスにログインします。
2. Cisco Defense OrchestratorのPoliciesメニューから、FTD Policiesを選択します。
3. FTDのPoliciesメニューから、Decryptionを選択します。
4. 適切な復号化ポリシーを選択します。
5. [編集（Edit）] アイコン（鉛筆の形）をクリックします。
6. Advanced Settingsタブをクリックします。
7. Enable TLS 1.3 Decryptionを無効にします。
8. [Save] をクリックします。

上記のポリシーを変更した後、新しいポリシーをFTDデバイスに展開します。

Cisco Defense Orchestratorによって管理されるデバイスの詳細については、Cisco Defense Orchestratorのドキュメントを参照してください。

TLS 1.3の復号化の詳細については、『Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator』の「Decryption Policy Advanced Options」セクションを参照してください。

Cisco Defense Orchestratorで管理されているCisco FDMデバイスのTLS 1.3復号化の詳細については、『Cisco Defense OrchestratorでのFDMデバイスの管理』の「SSL復号化ポリシー」セクションを参照してください。

これらの回避策と緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契

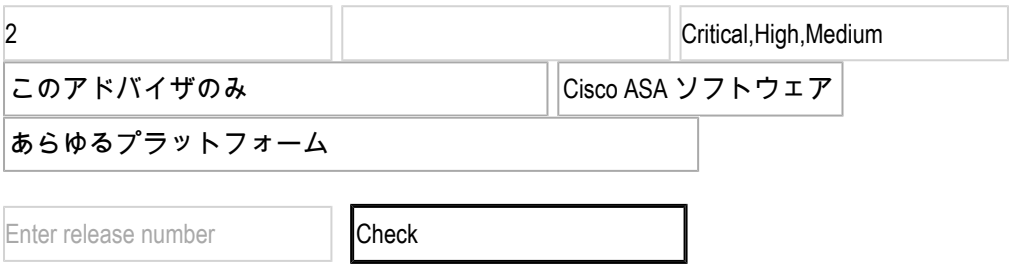
約しているメンテナンスプロバイダーにお問い合わせください。

Cisco ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスクを判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。すべてのアドバイザリ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、またはこのアドバイザリのみを選択します。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco ASA ソフトウェアの場合は 9.16.2.11、Cisco FTD ソフトウェアの場合は 6.6.7 と入力します。
5. [チェック（Check）] をクリックします。



関連情報

最適な Cisco ASA、FTD、または FMC ソフトウェアリリースの決定方法については、次の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco ASA の互換性
Cisco Secure Firewall ASA アップグレードガイド
Cisco Secure Firewall Threat Defense 互換性ガイド

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort3-uAnUntcV

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2023年11月1日

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。