CiscoFirepower脅威対策ソフトウェアのSSLおよびSnort 3検出エンジンにおけるバイパスとサービス妨害(DoS)の脆弱性

アドバイザリーID : cisco-sa-ftd-snort3-8U4HHxH8
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 : CSCwc07015

CVE-2023-20031

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

Snort 3 Detection EngineとCiscoFirepower脅威対策(FTD)ソフトウェアの統合におけるSSL/TLS証明書処理の脆弱性により、認証されていないリモートの攻撃者がSnort 3 Detection Engineの再起動を引き起こす可能性があります。

この脆弱性は、SSL接続を開始するときに、ロードされているSSL/TLS証明書にアクセスするときに発生する論理エラーが原因です。攻撃者は、特定の時間ベースの制約の下で、該当デバイスのSnort 3検出エンジンによる検査を受けるSSL/TLS接続要求を大量に送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はSnort 3検出エンジンのリロードを引き起こし、デバイスの設定に応じてバイパス状態またはサービス妨害(DoS)状態が発生する可能性があります。詳細については、このアドバイザリの「詳細」セクションを参照してください。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-snort3-8U4HHxH8

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

この脆弱性は、公開時点でCisco FTDソフトウェアが脆弱性のあるリリースを実行しており、次の条件をすべて満たしている場合に、ソフトウェアに影響を与えました。

- デバイスはSnort 3を実行していました。
- 次の条件のうち少なくとも1つが当てはまりました。
  - TLSサーバID検出が有効になりました。
  - SSLポリシーが設定されました。

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TLSサーバID検出設定の確認

TLSサーバID検出はデフォルトで無効になっています。

FTDソフトウェアCLIを使用したCisco FTDソフトウェアTLSサーバID検出設定の確認

Cisco FTDソフトウェアを実行しているデバイスでTLSサーバID検出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、show access-control-configコマンドを使用します。Advanced Settingsセクションまでスクロールします。コマンド出力に「TLS Server Identity Discovery Enabled」と表示された場合、デバイスは次の例に示すように、この脆弱性の影響を受けます。

```
<#root>

>

show  access-control-config

===============[ Advanced Settings ]================
General Settings
  Maximum URL Length                  : 1024
  Interactive Block Bypass Timeout    : 600
  SSL Policy                          : Certificate-Visibility-SSL-Policy
```

```
  TLS Server Identity Discovery       :
Enabled
```

次の例は、TLSサーバID検出が無効になっていることを示しています。

```
<#root>
>
show access-control-config
===============[ Advanced Settings ]================
General Settings
  Maximum URL Length                  : 1024
  Interactive Block Bypass Timeout    : 600
  TLS Server Identity Discovery       :
Disabled
```

注:CSCvz06256が原因で、このコマンドはCisco FTD 7.0ソフトウェアトレインのTLSサーバID検出設定を表示しません。

Cisco Device Managerソフトウェアで管理されるデバイスのCisco FTDFirepowerTLSサーバID検出設定の確認

TLSサーバID検出が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で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 FDM 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. Settings歯車アイコンをクリックします。
4. TLS Server Identity Discovery設定を見つけます。
    - 設定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。
    - この設定を無効にした場合、デバイスはこの脆弱性の影響を受けない可能性があります。

TLSサーバID検出の詳細については、『Firepower Device Manager用CiscoFirepower脅威対策コンフィギュレーションガイド』の「アクセスコントロール」の章を参照してください。

Cisco FTDFirepowerManagement Center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サーバID検出設定の確認

Cisco Server Management Center(FMC)ソフトウェアによって管理されているデバイスでTLSFirepowerID検出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 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. [詳細] タブをクリックします。
6. TLS Server Identity Discovery設定を見つけます。
    - 設定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。
    - この設定を無効にした場合、デバイスはこの脆弱性の影響を受けない可能性があります。

TLSサーバID検出の詳細については、『Cisco Secure Firewall Management Centerデバイス設定ガイド』の「アクセスコントロールポリシー」の章を参照してください。

Cisco Defense OrchestratorデバイスのCisco FTDソフトウェアTLSサーバID検出設定の確認

Cisco Defense Orchestratorソフトウェアで管理されているデバイスでTLSサーバIDディスカバリ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. Moreを選択し、次にAdvanced Settingsをクリックします。
7. TLS Server Identity Discovery設定を見つけます。
    - 設定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。
    - この設定を無効にした場合、デバイスはこの脆弱性の影響を受けない可能性があります。

TLSサーバID検出の詳細については、Cisco Defense Orchestratorのドキュメントを参照してください。

Cisco 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、次の例に示すとおり、この脆弱性の影響を受けます。

<#root>

```
>
show ssl-policy-config

==================[ CSCwc07015 ]==================
=================[ Default Action ]================
Default Action             : Do Not Decrypt
...
```

次の例では、SSLポリシーは適用されていません。

```
<#root>
>
show ssl-policy-config

SSL policy not yet applied
```

Cisco FDM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 FDMソフトウェアによって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 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。
    - Policy Nameがリストされている場合、デバイスはこの脆弱性の影響を受けます。
    - 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ない可能性があります。

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 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SSLポリシー設定の確認

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 FMC 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。
    - Policy Nameがリストされている場合、デバイスはこの脆弱性の影響を受けます。
    - Noneがリストされている場合、デバイスはこの脆弱性の影響を受けない可能性があります。

SSL復号化ポリシーの詳細については、『Cisco Secure Firewall Management Centerデバイス設定ガイド』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エリアを調べます。
    - Policy Nameがリストされている場合、デバイスはこの脆弱性の影響を受けます。
    - 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。

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。

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

詳細

次のCisco FTDソフトウェアSnort 3の設定パラメータは、Snort 3プロセスが再起動した場合のト

ラフィックの処理方法を制御します。これにより、この脆弱性のエクスプロイト中に暗号化されたトラフィックの処理方法が変更される可能性があります。

- Snortのフェールオープン
- Snortのpreserve-connection

firepower詳細については、『Firewall Management Center Configuration Guide』の「Snort Restart Traffic Behavior」セクション、または『Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator』ガイドを参照してください。

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、Snort 2に戻すか、Snort 3に残っている場合は、TLSサーバID検出と設定済みの復号化ポリシーの両方を無効にします。いずれかが有効になっている場合、そのデバイスはまだ脆弱です。

注：TLSサーバID検出を有効にするために、復号化ポリシーを設定してアクセスコントロールポリシーに関連付ける必要はありません。

Snort 2への復帰

Snort 2に戻る前に、『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」セクションにある「はじめる前に」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カスタマイズ、およびホスト名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。

CLIを使用したCisco FTDデバイスのSnort 2への復帰

CLIを使用してSnort 2に戻すオプションはありません。

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、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、『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、FTDデバイスに変更を展開します。

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。

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』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。

Cisco FDMソフトウェアによって管理されるデバイスの緩和策

Snort 3を使用しているCisco FTDデバイスでは、回避策を実装するために、TLSサーバID検出とSSLポリシーの両方を無効にする必要があります。1つの項目だけを無効にすると、デバイスは脆弱なままになります。

Cisco FDMソフトウェアによって管理されるデバイスのTLSサーバID検出を無効にするには、次の手順を実行します。

1. Cisco FDM 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. Settings歯車アイコンをクリックします。
4. TLSサーバID検出設定が有効になっている場合は、無効にしてOKをクリックします。

Cisco FDMソフトウェアで管理されているデバイスのSSLポリシーを無効にするには、次の手順を実行します。

1. Cisco FDM 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 Decryptionを選択します。
3. ポリシー名が存在する場合は、SSL復号化を無効にします。

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。

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「アクセスコントロール」の章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緩和策

回避策を実装するには、TLSサーバID検出とSSLポリシーの両方を無効にする必要があります。1つの項目だけを無効にすると、デバイスは脆弱なままになります。

正しい設定ページに移動して、Cisco FMCソフトウェアによって管理されているデバイスのポリシーを無効にするには、次の手順を実行します。

1. Cisco FMC 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. [詳細] タブをクリックします。

Cisco FMCソフトウェアで管理されているデバイスのTLSサーバID検出を無効にするには、次の手順を実行します。

1. TLSサーバのID検出設定を見つけます。
2. 設定が有効になっている場合は、鉛筆アイコンをクリックします。
3. Early application detection and URL categorizationボックスのチェックマークを外し、OKを選択します。
4. Saveをクリックして、ポリシーを保存します。

Cisco FMCソフトウェアで管理されているデバイスのSSLポリシーを無効にするには、次の手順を実行します。

1. SSLポリシー設定を見つけます。
2. ポリシー名が存在する場合は、編集鉛筆アイコンをクリックします。
3. ドロップダウンメニューでNoneを選択し、OKを選択します
4. Saveをクリックして、ポリシーを保存します。

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

詳細については、『Firepower Management Center Device Configuration Guide』の「Access Control」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緩和策

回避策を実装するには、TLSサーバID検出とSSLポリシーの両方を無効にする必要があります。1つの項目だけを無効にすると、デバイスは脆弱なままになります。

Cisco Defense Orchestratorソフトウェアで管理されているデバイスのポリシーを無効にするための正しい設定ページに移動するには、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. CDO Policiesメニューから、FTD Policiesを選択します。
3. FTD 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. Moreを選択し、Advanced Settingsをクリックします。

Cisco Defense Orchestratorソフトウェアで管理されているデバイスのTLSサーバID検出を無効にするには、次の手順を実行します。

1. TLSサーバのID検出設定を見つけます。
2. 設定が有効になっている場合は、鉛筆アイコンをクリックします。
3. Early application detection and URL categorizationボックスのチェックマークを外し、OKを選択します。
4. Saveをクリックして、ポリシーを保存します

Cisco Defense Orchestratorソフトウェアで管理されているデバイスのSSLポリシーを無効にする

には、次の手順を実行します。

1. 復号ポリシー設定を見つけます。
2. ポリシー名が存在する場合は、鉛筆アイコンをクリックします
3. ドロップダウンメニューでNoneを選択し、次にOKを選択します。
4. Saveをクリックして、ポリシーを保存します

上記のポリシーを変更した後、新しいポリシーをCisco Defense Orchestratorデバイスに展開します。

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。

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。

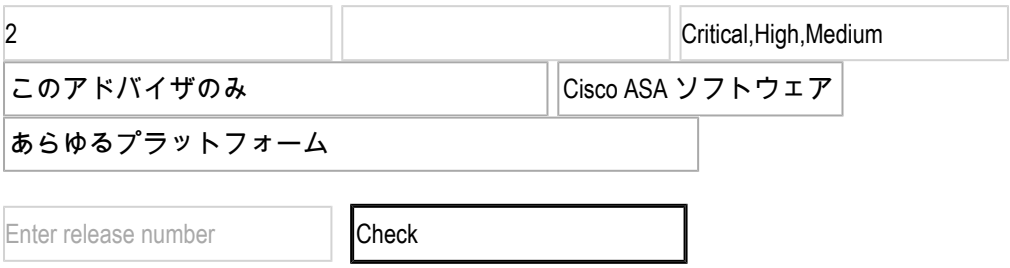
修正済みリリース

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。



FTD デバイスのアップグレード手順については、Cisco Firepower Management Center アップグレードガイドを参照してください。

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-

8U4HHxH8

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。