Cisco Firepower Threat DefenseソフトウェアのSSL/TLS URLカテゴリおよび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-sa-ftd-snort3-urldos-OccFQTeX
CVE-2023-20177
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 : CSCwe87591

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

SSL/TLS接続にURLカテゴリが設定されており、Snort 3検出エンジンが認証されていないリモートの攻撃者によってSnort 3検出エンジンが予期せず再起動させられる可能性がある場合、Cisco Firepower Threat Defense(FTD)ソフトウェアのSSLファイルポリシー実装における脆弱性が発生します。

この脆弱性は、Snort 3検出エンジンが、SSLファイルポリシーに設定されたURLカテゴリ、またはTLSサーバID検出が有効になっているアクセスコントロールポリシーに設定されたURLカテゴリを持つSSL/TLS接続を検査するときに発生する論理エラーが原因で存在します。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SSL/TLS接続を送信することで、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検出エンジンの予期しない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またはサービス拒否(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 3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-sa-ftd-

snort3-urldos-OccFQTeX

このアドバイザリは、2023 年 11 月に公開された Cisco ASA、FTD、および FMC のセキュリティ アドバイザリ バンドルに含まれています。アドバイザリとリンクの一覧については、Cisco Event Response：2023 年 11 月に公開された Cisco ASA、FMC、および FTD ソフトウェア セキュリティ アドバイザリ バンドル（半期）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影響を与えました。

- デバイスはSnort 3を実行していました。
- デバイスには、次の設定のうち少なくとも1つが含まれていました。
  - URLカテゴリが設定されたSSLポリシー。
  - TLSサーバIDディスカバリが有効で、URLカテゴリが設定されたアクセスコントロールポリシー。

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

Cisco FTDソフトウェアでSnort 3が実行されているかどうかを確認するには、「Firepower Threat Defense(FTD)で実行されるアクティブなSnort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がアクティブである必要があります。

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」と表示された場合、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ない可能性があります。

<#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、次の例に示すとおり、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


==================[ CSCwe87591 ]==================
================[ Default Action ]================
Default Action             : Do Not Decrypt
...
```

Cisco Firepower Device Manager(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SSLポリシー設定の確認

Cisco Firepower Device Manager(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ない可能性があります。
    - ポリシー名がリストされている場合、デバイスにはSSLポリシーが適用されており、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 Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「SSL復号化」の章を参照してください。

Cisco Firepower Management Center(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 Firepower Management Center(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. [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、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。
    - ポリシー名がリストされている場合、デバイスにはSSLポリシーが適用されており、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エリアを調べます。
    - 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。
    - ポリシー名がリストされている場合、デバイスにはSSLポリシーが適用されており、この脆弱性の影響を受ける可能性があります。

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「Decryption Policies」の章を参照してください。

Cisco Defense Orchestratorで管理する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』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SSLポリシーURLカテゴリ設定の確認

SSLポリシーのURLカテゴリは、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URLカテゴリ設定の確認

CLIを使用してデバイスにSSLポリシーのURLカテゴリ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、grep url /ngfw/var/sf/detection_engines/*/ssl/ssl.rulesコマンドを使用します。

コマンド出力にurl_categories (any)が表示される場合、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ない可能性があります。

```
<#root>

>

expert


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

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

url_categories (any);
```

コマンド出力にurl_categories(数字の文字列)が表示される場合、デバイスにはURLカテゴリが設定された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>

>

expert


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

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

url_categories (2107:0:0,2107:1:100);
```

Cisco FDM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URLカテゴリ設定の確認

Cisco FDMソフトウェアによって管理されているデバイスにURLカテゴ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 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. 設定されたルールごとに、URL列を確認します。
    - この列の値がANYの場合、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。
    - その列の値に他の値が含まれている場合、デバイスにはURLカテゴリが設定されたSSLポリシーがあり、この脆弱性の影響を受けます。

URLカテゴリの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「SSL復号化ルールのURL基準」セクションを参照してください。

URLフィルタリングの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Access Control」の章の「URL filtering」の項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URLカテゴリ設定の確認

Cisco FMCソフトウェアで管理されているデバイスにURLカテゴ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. FMC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. 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. 設定したルールごとに、[カテゴリ] 列を確認します。
    - この列の値がanyの場合、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。
    - その列の値に他の値が含まれている場合、デバイスにはURLカテゴリが設定されたSSLポリシーがあり、この脆弱性の影響を受けます。

URLカテゴリの詳細については、『Cisco Secure Firewall Management Centerコンフィギュレーションガイド』の「カテゴリルールの条件」セクションを参照してください。

URLフィルタリングの詳細については、『Cisco Secure Firewall Management Centerコンフィギュレーションガイド』の「アクセス制御」の章にある「URLフィルタリング」の項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URLカテゴリ設定の確認

Cisco Defense Orchestratorによって管理されるデバイスにURLカテゴ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、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. 設定したルールごとに、[カテゴリ] 列を確認します。
    - この列の値がanyの場合、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。
    - その列の値に他の値が含まれている場合、デバイスにはURLカテゴリが設定されたSSLポリシーがあり、この脆弱性の影響を受けます。

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。

URLカテゴリの詳細については、『Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator』の「Decryption Rules」の章を参照してください。

URLフィルタリングの詳細については、『Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator』の「Access Control」の章を参照してください。

Cisco Defense Orchestratorで管理するCisco FDMデバイスのURLカテゴリの詳細については、『Cisco Defense OrchestratorでのFDMデバイスの管理』の「SSL復号化ルールのURL基準」セクションを参照してください。

URLフィルタリングの詳細については、『Cisco Defense Orchestratorを使用したFDMデバイスの管理』の「アクセス制御」セクションを参照してください。

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ソフトウェアの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ダウンします。出力に「TLS Server Identity Discovery Enabled」と表示される場合、デバイスは次の脆弱性の影響を受ける可能性があります。

次の例は、TLSサーバIDディスカバリが無効になっていることを示しています。

<#root>

```
>
show access-control-config


===============[詳細設定]================
一般的な設定
 最大URL長：1024
 Interactive Block Bypass Timeout（インタラクティブブロックバイパスタイムアウト）:600
 TLSサーバIDディスカバリ： 無効
```

次の例は、TLSサーバID検出が有効になっていることを示しています。

```
<#root>
>
show access-control-config


===============[詳細設定]================
一般的な設定
 最大URL長：1024
 Interactive Block Bypass Timeout（インタラクティブブロックバイパスタイムアウト）:600
 SSLポリシー：Certificate-Visibility-SSL-Policy
 TLSサーバIDディスカバリ： 有効
```

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 FDM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サーバID検出設定の確認

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、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る可能性があります。
    - 設定が無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 Firepower Threat Defense Configuration Guide

for Firepower Device Manager』の「アクセス制御」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TLSサーバID検出設定の確認

Cisco FMCによって管理されているデバイスで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、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る可能性があります。
    - 設定が無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』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によって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 Defense Orchestratorによって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、Advanced Settingsの順にクリックします。
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る可能性があります。
    - 設定が無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ソフトウェアアクセスコントロールポリシーのURLカテゴリ設定の確

認

アクセスコントロールポリシーのURLカテゴリは、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ソフトウェアアクセスコントロールポリシーURLカテゴリ設定の確認

show access-control-configコマンドを使用します。Ruleセクションまでスクロールします。

コマンドの出力にcategoryセクションが含まれていない場合、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。次の例では、URLカテゴリが設定されていません。

```
<#root>

>

 show access-control-config


----------[ ルール:CSCwe87591_AC ]----------
   アクション：Fast-path
     ソースISEメタデータ：
   ソースゾーン：inside_zone
   宛先ゾーン：outside_zone
   ユーザ
   URL
   ロギングの設定
```

コマンドの出力にCategory: any valueと表示されている場合、デバイスはURLカテゴリが設定されているこの例に示すように、この脆弱性の影響を受ける可能性があります。

```
> show access-control-config


----------[ ルール:CSCwe87591_AC ]----------
   アクション：Fast-path
     ソースISEメタデータ：
   ソースゾーン：inside_zone
   宛先ゾーン：outside_zone
   ユーザ
   URL
    カテゴリ：ボットネット
    レピュテーション：不明
   ロギングの設定
```

Cisco FDMによって管理されるデバイスのCisco FTDソフトウェアアクセスコントロールポリシーURLカテゴリ設定の確認

Cisco FDMによって管理されているデバイスにアクセスコントロールポリシーURLカテゴ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 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. Access Controlタブを選択します。
4. 設定されたルールごとに、URL列を確認します。
    - この列の値がANYの場合、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。
    - その列の値に他の値が含まれている場合、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。

アクセスコントロールポリシーのURLカテゴリの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』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Cisco FTDソフトウェアアクセスコントロールポリシーURLカテゴリ設定の確認

Cisco FMCソフトウェアによって管理されるデバイスにアクセスコントロールポリシーURLカテゴ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 FMC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. [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. 設定したルールごとに、URL列を確認します。
    - この列の値がAnyの場合、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。
    - その列の値に他の値が含まれている場合、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。

アクセスコントロールポリシーのURLカテゴリの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「アクセスコントロール」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ソフトウェアアクセスコントロールポリシーURLカテゴリ設定の決定

Cisco Defense Orchestratorで管理されているデバイスにアクセスコントロールポリシーURLカテゴ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. 設定したルールごとに、URL列を確認します。
    - この列の値がAnyの場合、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。
    - その列の値に他の値が含まれている場合、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で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。

アクセスコントロールポリシーのURLカテゴリの詳細については、『Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator』の「アクセスコントロール」の章を参照してください。

アクセス制御ポリシーのURLカテゴリの詳細については、『Cisco Defense OrchestratorでのFDMデバイスの管理』の「アクセス制御」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

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
- オープンソースの Snort 2
- オープンソースの 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フェールオープン
- Snort preserve-connection（接続維持）

詳細については、『Firepower Management Centerコンフィギュレーションガイド』の「Snortのトラフィック再開動作」セクション、または『Cisco Defense Orchestratorでのクラウド配信ファイアウォール管理センターを使用したファイアウォール脅威対策の管理』ガイドを参照してください。

セキュリティ侵害の痕跡

この脆弱性が不正利用された可能性があるのは、特定のSnort 3カウンタが増加した場合です。管理者は、show snort counters CLIコマンドを発行して、rules_url_retryやcache_original_expireの0以外の値を検索できます。

```
<#root>

#

show snort counters

.
.
.

rules_url_retry

: 1676

cache_original_expire

: 124
.
.
.
#
```

これらのカウンタは、他の条件に対しても増加する可能性があります。さらにサポートが必要な場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

回避策

この脆弱性に対処する回避策と対応策があります。この脆弱性に対する攻撃ベクトルを削除するには、次のいずれかを実行します。

- Snort 2に戻します。
- Snort 3に残りますが、次のいずれかが設定されていないことを確認します。
    - URLカテゴリが設定されたSSLポリシー。
    - TLSサーバIDディスカバリが有効で、URLカテゴリが設定されたアクセスコントロールポリシー。

注：TLSサーバID検出を有効にするために、復号化ポリシーまたはSSL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に戻す

ダウングレードする前に、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Snort 2とSnort 3の間の切り替え」セクションの「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。展開への復帰の影響については、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を使用してこの設定を変更する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に戻す

Cisco FDMソフトウェア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 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、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』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に戻す

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ソフトウェアの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、Cisco FTDデバイスに変更を導入します。

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によって管理されるCisco FTDデバイスのSnort 2に戻す

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によって管理される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管理対象デバイスの対応策

Snort 3を使用しているCisco FTDデバイスでは、デバイスがこの脆弱性の影響を受けないように、アクセスコントロールポリシーとSSLポリシーの両方をチェックする必要があります。どちらかの場所が脆弱な方法で設定されている場合、そのデバイスはこの脆弱性の影響を受けます。

アクセス コントロール ポリシー

デバイスでTLSサーバIDディスカバリが有効になっており、URLカテゴリが設定されたアクセスコントロールポリシーが使用されている場合、そのデバイスはこの脆弱性の影響を受けます。次のオプションを使用して、攻撃ベクトルを閉じることができます。

1. TLSサーバID検出を無効にし、URLカテゴリは設定したままにします。
2. URLカテゴリの設定を削除し、TLSサーバIDを有効のままにします。

SSLポリシー

デバイスでURLカテゴリが設定されたSSLポリシーが使用されている場合、そのデバイスはこの脆弱性の影響を受けます。次のオプションを使用して、攻撃ベクトルを閉じることができます。

1. SSLポリシーからURLカテゴリの設定を削除します。

2. アクセスコントロールポリシーからSSLポリシーを削除します。

TLSサーバID検出の無効化

CLIを使用したTLSサーバID検出の無効化Cisco FTDデバイス

CLIを使用してこの設定を変更するオプションはありません。

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検出の無効化

Cisco FDMソフトウェア管理デバイスの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検出の設定が有効になっている場合は、その設定を無効にして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。

詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Access Control」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TLSサーバID検出の無効化

Cisco FMC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 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。
7. 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。
8. Early application detection and URL categorizationボックスのチェックマークを外して、OKを選択します。
9. 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デバイス設定ガイド』の「アクセス制御」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に対してCiscoのTLSサーバID検出を無効にする

Cisco Defense Orchestrator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. 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の順にクリックします。
7. TLS Server Identity Discovery設定を見つけます。
8. 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。
9. Early application detection and URL categorizationボックスのチェックマークを外して、OKを選択します。
10. 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。

Cisco Defense Orchestratorで管理されるCisco FMCデバイスのTLSサーバID検出の詳細については、『Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator』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で管理されるCisco FDMデバイスのTLSサーバID検出の詳細については、『Cisco Defense OrchestratorでのFDMデバイスの管理』の「FDM管理対象デバイスの設定」セクションを参照してください。

アクセス制御ポリシーURLカテゴリの削除

CLIを使用したCisco FTDデバイスのアクセスコントロールポリシーURLカテゴリの削除

CLIを使用してこの設定を変更するオプションはありません。

FDMソフトウェアによって管理されるCisco FTDデバイスのアクセス制御ポリシーURLカテゴリの削除

Cisco FDMソフトウェアによって管理されるデバイスのアクセスコントロールポリシーURLカテゴリを無効にするには、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. メインメニューから [ポリシー（Policies）] を選択します。

3. Access Controlタブを選択します。
4. 設定されたルールごとに、URL列を確認します。
5. カテゴリが表示されている場合は、カテゴリの名前をクリックします。
6. ポップアップウィンドウで、名前の横にあるXをクリックしてカテゴリを削除し、「OK」を選択します。

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。

アクセスコントロールポリシーのURLカテゴリの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「アクセスコントロール」の章を参照してください。

FMCソフトウェアによって管理されるCisco FTDデバイスのアクセスコントロールポリシーURLカテゴリの削除

Cisco FMCソフトウェアで管理されているデバイスのアクセスコントロールポリシーURLカテゴリを無効にするには、次の手順を実行します。

1. Cisco FMCソフトウェアの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. 設定したルールごとに、URL列を確認します。
6. カテゴリが表示されている場合は、カテゴリの名前をクリックします。
7. ポップアップウィンドウでごみ箱アイコンをクリックしてURLカテゴリを削除し、Saveを選択します。
8. Saveを選択します。

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。

アクセスコントロールポリシーのURLカテゴリの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「アクセスコントロール」の章を参照してください。

Cisco Defense Orchestratorによって管理されるCisco FTDデバイスのアクセスコントロールポリシーURLカテゴリの削除

Cisco Defense Orchestratorで管理されているデバイスのアクセスコントロールポリシーURLカテゴリを無効にするには、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、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. 設定したルールごとに、URL列を確認します。
7. カテゴリが表示されている場合は、カテゴリの名前をクリックします。
8. ポップアップウィンドウで、名前の横にあるXをクリックしてカテゴリを削除し、「適用」を選択します。
9. Saveを選択します。

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。

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。

アクセスコントロールポリシーのURLカテゴリの詳細については、『Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator』の「Access Control」の章を参照してください。

アクセス制御ポリシーのURLカテゴリの詳細については、『Cisco Defense OrchestratorによるFDMデバイスの管理』ガイドの「アクセス制御」セクションを参照してください。

SSLポリシーURLカテゴリを削除しています

CLIを使用したCisco FTDデバイスのSSLポリシーURLカテゴリの削除

CLIを使用してこの設定を変更するオプションはありません。

FDMソフトウェアによって管理されているCisco FTDデバイスのSSLポリシーURLカテゴリの削除

Cisco FDMソフトウェアによって管理されているデバイスのSSLポリシーURLカテゴリ設定を削除するには、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. 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. 設定されたルールごとに、URL列を確認します。
5. カテゴリが表示されている場合は、カテゴリの名前をクリックします。
6. ポップアップウィンドウで、カテゴリ名の横にあるXをクリックして、カテゴリを削除します
7. [OK] を選択します。

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。

URLカテゴリの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「SSL復号化ルールのURL基準」セクションを参照してください。

URLフィルタリングの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Access Control」の章の「URL filtering」セクションを参照してください。

FMCによって管理されるCisco FTDデバイスのSSLポリシーURLカテゴリの削除

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URLカテゴリ設定を削除するには、次の手順を実行します。

1. Cisco FMC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. 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. 設定したルールごとに、[カテゴリ] 列を確認します。
6. カテゴリが表示されている場合は、カテゴリの名前をクリックします。
7. ポップアップウィンドウでごみ箱アイコンをクリックしてURLカテゴリを削除し、Saveを選択します。
8. Saveを選択します。

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。

URLカテゴリの詳細については、『Cisco Secure Firewall Management Centerコンフィギュレーションガイド』の「カテゴリルールの条件」セクションを参照してください。

URLフィルタリングの詳細については、『Cisco Secure Firewall Management Centerコンフィギュレーションガイド』の「アクセス制御」の章で、「URLフィルタリング」の項を参照してください。

Cisco Discovery Orchestratorによって管理されるCisco FTDデバイスのSSLポリシーURLカテゴリの削除

Cisco Discovery Orchestratorで管理されているデバイスのSSLポリシーURLカテゴリの設定を削除するには、次の手順を実行します。

1. Cisco Discovery Orchestrator Webインターフェイスにログインします。
2. Cisco Discovery 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. 設定したルールごとに、URL列を確認します。
7. カテゴリが表示されている場合は、カテゴリの名前をクリックします。
8. ポップアップウィンドウで、ゴミ箱アイコンをクリックしてカテゴリを削除し、「保存」を選択します。
9. Saveを選択します。

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。

Cisco Discovery 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。

URLカテゴリの詳細については、『Cisco Defense Orchestratorガイド』の「Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center」の「Decryption Rules」の章を参照してください。

URLフィルタリングの詳細については、『Cisco Defense Orchestratorガイド』の「Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center」の「Access Control」の章を参照してください。

Cisco Discovery Orchestratorで管理するCisco FDMデバイスのURLカテゴリの詳細については、『Cisco Defense OrchestratorでのFDMデバイスの管理』の「SSL復号化ルールのURL基準」セクションを参照してください。

URLフィルタリングの詳細については、『Cisco Defense Orchestratorを使用したFDMデバイスの管理』の「アクセス制御」セクションを参照してください。

アクセスコントロールポリシーからのSSLポリシーの削除

CLIを使用したCisco FTDデバイスのアクセスコントロールポリシーからのSSLポリシーの削除

CLIを使用してこの設定を変更するオプションはありません。

FDMソフトウェアによって管理されるCisco FTDデバイスのアクセス制御ポリシーからのSSLポリシーの削除

Cisco FDMソフトウェアによって管理されているデバイスのSSLポリシーURLカテゴリ設定を削除するには、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. 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が有効になっている場合は、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FTDデバイスに展開します。

SSL復号化の詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「SSL復号化」の章を参照してください。

FMCによって管理されるCisco FTDデバイスのアクセスコントロールポリシーからのSSLポリシーの削除

Cisco FDMソフトウェアによって管理されているデバイスのSSLポリシーURLカテゴリ設定を削

除するには、次の手順を実行します。

1. Cisco FMC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. [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。
6. ポリシー名が表示されている場合は、名前をクリックします。
7. ポップアップウィンドウで、ドロップダウンメニューからNoneを選択し、OKを選択します。
8. Saveを選択します。

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。

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 Discovery Orchestratorによって管理されるCisco FTDデバイスのアクセスコントロールポリシーからのSSLポリシーの削除

Cisco Discovery Orchestratorで管理されているデバイスのSSLポリシーURLカテゴリの設定を削除するには、次の手順を実行します。

1. Cisco Discovery Orchestrator Webインターフェイスにログインします。
2. Cisco Discovery 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領域を調べます。
7. ポップアップウィンドウにポリシー名がある場合は、ドロップダウンメニューからNoneを選択し、Applyを選択します。
8. Saveを選択します。

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。

2		Critical,High,Medium
このアドバイザのみ	Cisco ASA ソフトウェア	
あらゆるプラットフォーム		
Enter release number	Check	

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-sa-ftd-snort3-urldos-OccFQTeX

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。