Cisco適応型セキュリティアプライアンスソフトウェアおよびFirepower Threat Defenseソフトウェアのトラストポイント設定のデフォルト

Advisory ID : cisco-sa-racerts-WvuYpxew
初公開日 : 2020-07-31 16:00
最終更新日 : 2020-07-31 22:35
バージョン 1.1 : Final
回避策 : Yes
Cisco Bug ID : CSCvv11100 CSCvt50528 CSCvv11051

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

Cisco適応型セキュリティアプライアンス(ASA)ソフトウェアおよびCisco Firepower Threat Defense(FTD)ソフトウェアは、リモートアクセスVPNの導入で証明書認証を設定できます。

外部の研究者が、誤って設定されたCisco ASAおよびFTDソフトウェアリモートアクセスデバイスをいくつか特定しました。このデバイスでは、VPNエンドポイントが同じパブリックCAから発行されたサーバID証明書を持つように設定されている場合、パブリック認証局(CA)からの有効な証明書を所有するユーザにVPNリモートアクセスを許可する可能性があります。

Cisco ASAとFTDソフトウェアがインポートされた証明書のトラストポイントにデフォルト設定を適用する方法と、トラストポイントが目的の機能だけに設定されていることを確認する方法に関して、お客様の関心を高めたいと考えています。

Cisco ASAまたはFTDソフトウェアの脆弱性やデジタル証明書認証機能は考慮されませんが、設定の問題は考慮されます。

Cisco Adaptive Security Device Manager(ASDM)、Cisco Security Manager、およびCisco Firepower Management Center(FMC)を含むCisco ASAおよびFTDソフトウェアの今後のリリースでは、証明書をインポートする際に警告アラートが生成され、デフォルトの動作をお客様に通知します。また、Cisco Bug ID CSCvt50528、CSCvv11100、およびCSCvv11051で設定を強化する方法についてのガイダンスも提供されます。

ただし、適切な強化処理を行うために、これらのCisco Bug IDと統合されたコードを実行することは要件ではありません。このアドバイザリを確認し、それぞれの設定変更を行うことをお勧め

します。

詳細

この情報アドバイザリの対象読者は、リモートアクセスVPNエンドポイントとしてCisco ASA/FTDデバイスを導入し、クライアントベースの証明書認証を実行しているお客様です。

新しい証明書を設定にインポートする際、トラストポイントの使用に関するデフォルト設定はipsec-clientおよびssl-clientの検証に使用されるため、デフォルトでは、そのトラストポイントを使用してVPNユーザを認証できます。トラストポイントをサーバID証明書としてのみ使用し、対応する認証局(CA)の信頼をVPNの検証に使用しない場合、ASA/FTDの管理者はvalidation-usageコマンドを使用して、そのようなデバイスを設定する必要があります。

設定を変更せずに、他の認証および許可方式を使用せずにクライアント証明書認証を使用する場合、ASA/FTDデバイスのID証明書と同じ認証局によって発行された任意のユーザID証明書を使用して認証できる可能性があります。追加の認証と認可を使用するインストールでは、ネットワークへのアクセスを許可する前に追加の手順を渡すことを防止するか、または要求することになります。

推奨事項

確認方法

トラストポイントの設定はすべて見直して、目的に合わせて設定されていることを確認する必要がありますが、主なリスクは次のものを使用する場合です。

- リモートアクセスVPNエンドポイントとしてのASA/FTDデバイス。
- 認証局Aによって証明書が発行されるクライアント証明書認証。
- 認証局Bによって発行されたASA/FTDデバイスのIDの証明書。

この目的は、ASA/FTD VPNエンドポイントの管理者が、認証局Aによって発行されたクライアント証明書のみを考慮することです。たとえば、クライアントが発行した証明書は会社のプライベートCA(CA A)から発行され、ASA/FTD ID証明書はパブリックCA(CA B)から発行された可能性があります。

Cisco ASAまたはFTDデバイスがこのアドバイザリに記載された問題の影響を受けるかどうかを確認するには、次の手順に従います。

1)デバイスがリモートアクセスVPNを許可するように設定されているかどうかを確認します。

Cisco ASAの機能	識別設定
AnyConnect IKEv2 Remote Access（クライアントサービスあり）	crypto ikev2 enable <interface_name> client-services port <port #>
AnyConnect SSL VPN（トンネルモード）	webvpn

Cisco ASAの機能	識別設定
	<interface_name>を有効にします。
クライアントレス SSL VPN	webvpn <interface_name>を有効にします。

または、FMCで、Devices -> VPN -> Remote Accessの順に選択し、プロファイルが存在するかどうかを確認します。

有効になっている場合は、次の手順に進みます。

2)クライアント証明書認証を使用しているかどうかを確認します。

管理者はASA CLIまたはFTD CLIからshow running-config all tunnel-groupコマンドを使用して、証明書が含まれている認証方式が接続プロファイルで使用されているかどうかを確認できます。認証、許可、アカウンティング(AAA)またはSecurity Assertion Markup Language(SAML)2.0のいずれかの方式だけを使用する場合、デバイスは影響を受けません。次に、AAAとクライアント証明書認証の両方を使用しているASAデバイスでのコマンドの出力例を示します。

```
<#root>

ciscoasa#

show running-config all tunnel-group

 authentication aaa certificate
.
```

または、FMCで、Devices -> VPN -> Remote Accessの順に選択し、Remote Access profile nameをクリックします。異なる接続プロファイルの場合は、AAA列を確認します。Authenticationフィールドのいずれかが**Client Certificate Only**または**Client Certificate & AAA**を示している場合は、クライアント証明書が使用されています。次の手順に進みます。

注：別の認証方式を設定した場合でも、認証を渡すためにこれらの認証方式を満たし、ネットワークへのアクセスを許可する必要があります。

3)管理者が制御していない認証局によって発行されたASA/FTDのIDに証明書を使用しているかどうかを確認します。

管理者はまず、show running-config ssl | include trust-pointコマンドを使用して、リモートアクセスVPN対応インターフェイスで使用されているデバイスのID証明書を識別します。

```
<#root>

ciscoasa#
```

```
show running-config ssl | include trust-point

ssl trust-point IDENTITY outside
```

前記の例では、outsideという名前のインターフェイスが、IDENTITYという名前のトラストポイント内に設定されたID証明書に関連付けられています。

管理者は、このトラストポイントに含まれている証明書を表示し、特にCA証明書のサブジェクト名を確認することで、この証明書がパブリックCAによって発行されたかどうかを確認できます。

```
<#root>

ciscoftd#

show crypto ca certificate IDENTITY

Certificate

  .
  .


Issuer Name

:
  l=Sydney
  c=AU
  o=GoDaddy.com\, Inc.
  ou=http://certs.godaddy.com/repository/


cn=Go Daddy Secure Certificate Authority - G2
  Subject Name:

  .
  .
    cn=FPR2100-FTD

  Validity Date:
    start date: 07:16:53 UTC Jul 26 2020
    end   date: 07:16:53 UTC Jul 26 2021
  Storage: config


  Associated Trustpoints: FPR2100-FTD.cisco.com
```

または、FMCで、Devices -> VPN -> Remote Accessの順に選択し、Remote Access profile nameをクリックします。Access Interfacesをクリックします。これにより、リモートアクセスVPNインターフェイスのSSLグローバルID証明書フィールドに表示されるID証明書が表示されます。

修復

新しい証明書を設定にインポートする際、トラストポイントの使用に関するデフォルト設定はipsec-clientおよびssl-clientの検証に使用されるため、デフォルトでは、そのトラストポイントを使用してVPNユーザを認証できます。管理者は、すべてのトラストポイントの使用設定を確認する必要があります。トラストポイントがサーバ認証用の証明書を保持している場合、そのトラストポイントはvalidation-usage ssl-server設定コマンドを使用して設定する必要があります。クライアント認証に明示的に使用されていないトラストポイントには、次の手順に従ってno validation-usage設定を適用する必要があります。

ASAの場合、管理者はデバイスにログインし、validation-usageコマンドを使用してトラストポイントを再設定できます。

```
crypto ca trustpoint <name of identity trustpoint>
 no validation-usage
```

FMCを介して管理されるFTDの場合、管理者はFlexConfigを使用できます。次の手順を実行します。

1. show running-config all crypto ca trustpoint FTD CLIコマンドを使用して、再設定が必要なトラストポイントの設定を検証し、validation-usageがipsec-client ssl-clientに設定されていることを確認します。

2. FMCで、Objects -> Object Management -> FlexConfig -> FlexConfig Objectの順に移動し、NameフィールドとDescriptionフィールドに入力します。次の例に示すように、コマンドを使用してテキストボックスに入力します。TrustPointNameを変数として定義することも、変更するTrustPointNameの名前だけを入力することもできます。

```
Name: NoValidationUsage
Description: no validation-usage ipsec-client ssl-client
Text Box:
crypto ca trustpoint TrustPointName
no validation-usage
```

3. Devices -> FlexConfigの順に選択して、該当するデバイスにFlexConfigを適用します。

4. New Policyをクリックし、名前を作成し、ポリシーを割り当てるデバイスを選択します。次の画面でAdd FlexConfig Objectを選択し、前の手順で作成したオブジェクト（この例ではNoValidationUsage）をクリックします。

5. FlexConfigを保存します。

6. FlexConfigを導入します。

7. デバイスにログインし、show running-config all crypto ca trustpoint FTD CLIコマンドを発行して、設定が成功したことを検証します。パブリックトラストポイントでは、no validation-usageと表示される必要があります。

クライアント証明書がID証明書とは異なるCAから発行された場合でも、そのトラストポイントには、設計上の使用方法に応じて、validation-usage ipsec-client ssl-clientまたはvalidation-usage ssl-clientのいずれかをデフォルト設定で指定する必要があります。

Firepower Device Management(FDM)で管理されるFTDでは、現在、FlexConfigでトラストポイントの設定を変更する方法はありません。トラストポイントを再設定する機能をサポートする新しいバージョンがリリースされる予定です。

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

この問題を報告していただいたCenturyLink社のMike Guy氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-racerts-WvuYpxew

改訂履歴

バージョン	説明	セクション	Status	日付
1.1	外部の電子メール通知の再発行。	—	Final	2020年7月31日
1.0	初版リリース	—	Final	2020年7月31日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザーを対象としています。

該当製品

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。

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。