Cisco適応型セキュリティアプライアンスおよびFirepower Threat Defenseソフトウェアのリモートアクセス VPNのブルートフォースにおけるDoS脆弱性

アドバイザリーID : cisco-sa-asaftd-bf-dos-vDZhLqrW
CVE-2024-20481
初公開日 : 2024-10-23 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCwj45822 CSCwj91570

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

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)ソフトウェアのリモートアクセスVPN(RAVPN)サービスの脆弱性により、認証されていないリモート攻撃者がRAVPNサービスのサービス妨害(DoS)を引き起こす可能性があります。

この脆弱性は、リソースの枯渇が原因です。攻撃者は、該当デバイスに大量のVPN認証要求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、攻撃者はリソースを枯渇させ、該当デバイスでRAVPNサービスのDoSを引き起こす可能性があります。攻撃の影響によっては、RAVPNサービスを復元するためにデバイスのリロードが必要になる場合があります。VPNに関連しないサービスは影響を受けません。

Cisco Talosは、ブログ投稿『一般的に使用されるログインクレデンシャルを使用した、VPNやSSHサービスを対象とした大規模な総当たり攻撃』でこれらの攻撃について説明しています。

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。この脆弱性に対処する回避策はありません。

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-asaftd-bf-dos-vDZhLqrW

このアドバイザリは、2024年10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の一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco ASA、FMC、およびFTDソフトウェアに関するセキュリティアドバイザリ公開半年刊2024年10月』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 ASAまたは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て、RAVPNサービスが有効になっているシスコ製品に影響を与えました。

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。

SSL VPN 設定の確認

SSL VPNが有効になっているかどうかを確認するには、show running-config webvpn | include ^ enableコマンドをデバイスのCLIで使用します。次に、show running-config webvpn | include ^ enableコマンドを、外部インターフェイスでSSL VPNが有効になっているデバイスで使用します。

<#root>

```
firewall#
show running-config webvpn | include ^ enable


enable
 outside
```

コマンドの出力がない場合、SSL VPNはどのインターフェイスでも有効になっておらず、デバイスはこの脆弱性の影響を受けません。

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シスコ製品には影響を与えないことを確認しました。

- IOS ソフトウェア

- IOS XE ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア
- Secure Firewall Management Center(FMC)ソフトウェア（旧称：Firepower Management Center Software）

セキュリティ侵害の痕跡

デバイスがパスワードのスプレー攻撃を受けている場合、いくつかの潜在的なインジケータがあります。

最も一般的なインジケータは、頻繁かつ大量に発生する特定のログメッセージです。次に、パスワードスプレー攻撃中に表示される可能性のあるログメッセージのタイプの例を示します。どのメッセージが表示されるかはデバイスの設定によって異なるため、すべてのメッセージタイプがパスワードスプレー攻撃を示す必要はありません。

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = *10.1.2.3* : user = *admin* : user IP =

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database : user = *admin* : user

%ASA-6-716039

: Group <*DfltGrpPolicy*> User <*admin*> IP <*192.168.1.2*> Authentication: rejected, Session Type: WebVPN.

注：デバイスの設定によっては、ユーザ名を非表示にするために、ユーザ名フィールドに *文字が含まれる場合があります。

パスワードスプレー攻撃を検出するもう1つの方法は、認証要求と認証拒否の量を監視することです。そのためには、CLIでshow aaa-serverコマンドを複数回発行し、コマンドを使用する間隔を数秒にします。認証の拒否が大量に発生している場合は、攻撃が継続している可能性があります。次のshow aaa-serverコマンドの出力では、このコマンドを使用する間に認証要求と認証拒否の数が増加していることが示されています。

<#root>

Firewall#

show aaa-server

```
Server Group: LDAP-SERVER
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.1.2.3
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
```

Number of authentication requests 2220000

```
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
```

Number of rejects 2212345

```
Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
Firewall#
.
Wait some amount of time
.
Firewall#
```

show aaa-server

```
Server Group: LDAP-SERVER
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.1.2.3
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
```

Number of authentication requests 2234567

```
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
```

Number of rejects 2223456

```
Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
Firewall#
```

回避策

この脆弱性に対処する回避策はありません。ただし、パスワードスプレー攻撃を受けており、修正済みリリースにアップグレードしていないユーザのために実装できる緩和策があります。これらの緩和策については、『セキュアファイアウォールのリモートアクセスVPNサービスを対象としたパスワードスプレー攻撃に対する推奨事項』TechNoteで説明されています。

これらの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	

注：Cisco ASAソフトウェアを実行しているCisco 3000シリーズ産業用セキュリティアプライアンス(ISA)については、Cisco ASAソフトウェアリリース9.16.4.67のリリースは延期されており、リリース9.16.4.70に置き換えられています。

Cisco FTDデバイスのアップグレード手順については、該当する『Cisco FMC upgrade guide』を参照してください。

関連情報

最適な Cisco ASA、FMC、または FTD 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

推奨事項

修正済みリリースのインストール後は、『Cisco Secure Firewall ASA Firewall CLIコンフィギュレーションガイド』の「VPNサービスの脅威検出の設定」セクションを参照することをお勧めします。このセクションでは、RAVPNログイン認証攻撃、クライアント開始攻撃、および無効なVPNサービスへの接続試行からの保護を有効にする方法について説明します。必要な保護は、お客様の判断で決定します。

不正利用事例と公式発表

Cisco Product Security Incident Response Team(PSIRT)では、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を確認しています。

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-asaftd-bf-dos-vDZhLqrW

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	2024年10月23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。