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脅威対策ソフトウェアのリモートアクセスVPNの不正アクセスの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-ravpn-auth-8LyfCkeC　CVE-2023-20269
初公開日 : 2023-09-06 16:00
最終更新日 : 2023-10-11 14:59
バージョン 1.4 : Final
CVSSスコア : 5.0
回避策 : Yes
Cisco バグ ID : CSCwh23100 CSCwh45108

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CiscoFirepower脅威対策(FTD)ソフトウェアのリモートアクセスVPN機能の脆弱性により、認証されていないリモートの攻撃者がブルートフォース攻撃を実行して有効なユーザ名とパスワードの組み合わせを特定したり、認証されたリモートの攻撃者が不正ユーザとのクライアントレスSSL VPNセッションを確立したりする可能性があります。

この脆弱性は、リモートアクセスVPN機能とHTTPS管理およびサイト間VPN機能との間での認証、許可、アカウンティング(AAA)の不適切な分離に起因します。攻撃者は、総当たり攻撃を行う際、または有効なクレデンシャルを使用してクライアントレスSSL VPNセッションを確立する際に、デフォルトの接続プロファイルまたはトンネルグループを指定することで、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、攻撃者は次のいずれかまたは両方を達成できる可能性があります。

- 不正なリモートアクセスVPNセッションの確立に使用できる有効なクレデンシャルを特定します。
- クライアントレスSSL VPNセッションを確立します（Cisco ASAソフトウェアリリース9.16以前を実行している場合のみ）。

注：

- クライアントベースのリモートアクセスVPNトンネルを確立することはできません。これは

、これらのデフォルトの接続プロファイルやトンネルグループにはIPアドレスプールが設定されておらず、設定できないためです。
- この脆弱性では、攻撃者が認証をバイパスすることはできません。リモートアクセスVPNセッションを正常に確立するには、有効な資格情報が必要です。これには、多要素認証(MFA)が構成されている場合の有効な2番目の要素が含まれます。

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。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-asaftd-ravpn-auth-8LyfCkeC

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のあるリリースを実行しているシスコデバイスに影響を与えました。デバイスが脆弱かどうかを判断するための正確な条件は、以下に詳述するように、望ましい結果によって異なります。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

ブルートフォースアタック

ブルートフォースアタックは、次の両方の条件が満たされている場合に実行できます。

- 少なくとも1人のユーザがLOCALデータベースでパスワードを使用して設定されているか、有効なAAAサーバを指し示すまたはHTTPS管理認証が設定されています。
- SSL VPNが少なくとも1つのインターフェイスで有効になっているか、IKEv2 VPNが少なくとも1つのインターフェイスで有効になっている。

ブルートフォース攻撃に成功すると、攻撃者は不正なリモートアクセスVPNセッションを確立できるようになります。

不正なクライアントレスSSL VPNセッションの確立

クライアントレスSSL VPNセッションを正常に確立するには、次のすべての条件を満たす必要があります。

- 攻撃者は、LOCALデータベースまたは HTTPS管理認証に使用されるAAAサーバに存在するユーザの有効なクレデンシャルを持っています。これらのクレデンシャルは、総当た

り攻撃テクニックを使用して取得できます。
- デバイスでCisco ASAソフトウェアリリース9.16以前が実行されている。
- SSL VPNが少なくとも1つのインターフェイスで有効になっている。
- クライアントレスSSL VPNプロトコルはDfltGrpPolicyで許可されます。

注：Cisco FTDソフトウェアはクライアントレスSSL VPN機能をサポートしていないため、この攻撃は成功しません。

デバイス設定の確認

デバイス上のLOCALデータベース、HTTPS管理認証、IKEv2 VPN、SSL VPN、およびクライアントレスSSL VPNプロトコルの設定を確認するには、次の手順を使用します。

ローカルユーザデータベースの評価

show running-config username | include password CLIコマンドを使用して、パスワードが設定されたローカルユーザがLOCALデータベースに存在するかどうかを確認します。このコマンドの空でない出力は、パスワードを持つユーザが少なくとも1人設定されていることを示します。このコマンドの出力が空の場合は、パスワードが設定されたユーザが設定されていないことを示しています。

デフォルトでは、LOCALユーザデータベースは空です。

HTTPS管理認証設定の評価

show running-config aaa authentication | | include http CLIコマンドを使用して、HTTPS管理認証が有効なAAAサーバを指しているかどうかを確認します。次に、show running-config aaa authentication | | include httpコマンドを、HTTPS管理認証のためにAAAサーバのISEを指すデバイスで実行した場合の出力例を示します。

```
<#root>

asa#

show running-config aaa authentication | include http


aaa authentication http console

 ISE
```

次の例は、LOCALデータベースをポイントするデバイス上でこのコマンドを実行した場合の出力を示しています。

```
<#root>
```

```
asa#
show running-config aaa authentication | include http


aaa authentication http console
 LOCAL
```

HTTPS管理認証はデフォルトでは設定されていません。

注：

- Cisco ASAソフトウェアを実行している場合、aaa authentication http consoleコマンドでAAAサーバとローカルの両方をリストすることもできます。この場合、設定されたAAAサーバに到達できない場合は、LOCALデータベースだけが使用されます。
- Cisco FTDソフトウェアを実行している場合、aaa authentication http console aaa_serverコマンドはFlexConfigのみを使用してプッシュでき、LOCALオプションはリリース7.0以降でのみサポートされています。

IKEv2 VPN設定の評価

show running-config crypto ikev2 | include crypto ikev2 enable CLIコマンドを使用して、任意のインターフェイスでIKEv2 VPNが有効になっているかどうかを確認します。このコマンドの空でない出力は、リストされたインターフェイスでIKEv2 VPNが有効になっていることを示します。空の出力は、IKEv2 VPNがどのインターフェイスでも有効になっていないことを示します。

次に、show running-config crypto ikev2 | include crypto ikev2 enableコマンドを、outsideインターフェイスでIKEv2 VPNが有効になっているデバイスで実行した場合の出力例を示します。

```
<#root>
asa#
show running-config crypto ikev2 | include crypto ikev2 enable


crypto ikev2 enable
 outside
```

IKEv2 VPNは、デフォルトではどのインターフェイスでも有効になっていません。

注：crypto ikev2 enableコマンドでは、オプションのportパラメータを含む追加のclient-servicesオプションを指定できます。これらのオプションは、この脆弱性に関するデバイスの

ステータスには影響しません。

SSL VPN設定の評価

show running-config webvpn | include ^ enable CLIコマンドを使用して、任意のインターフェイスでSSL VPNが有効になっているかどうかを確認できます。このコマンドの出力が空でない場合は、リストされているインターフェイスでSSL VPNが有効になっていることを示します。出力が空の場合は、どのインターフェイスでもSSL VPNが有効になっていないことを示しています。

次に、show running-config webvpn | include ^ enableコマンドを、outside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実行した場合の出力例を示します。

```
<#root>

asa#

show running-config webvpn | include ^ enable


enable

 outside
```

SSL VPNは、デフォルトではどのインターフェイスでも有効になっていません。

クライアントレスSSL VPNプロトコル設定の評価

show running-config all group-policy DfltGrpPolicy | include vpn-tunnel-protocol CLIコマンドを使用して、クライアントレスSSL VPNプロトコルがDfltGrpPolicyで許可されているかどうかを確認します。次の例に示すように、このコマンドの出力にssl-clientlessが含まれている場合は、クライアントレスSSL VPNプロトコルが許可されます。

```
<#root>

asa#

show running-config all group-policy DfltGrpPolicy | include vpn-tunnel-protocol


 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec

ssl-clientless
```

クライアントレスSSL VPNプロトコルは、デフォルトでDfltGrpPolicyで許可されます。

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。

- Firepower Management Center（FMC）ソフトウェア
- FXOS ソフトウェア
- IOS ソフトウェア
- IOS XE ソフトウェア
- IOS XR ソフトウェア
- NX-OS ソフトウェア

セキュリティ侵害の痕跡

この脆弱性の侵害のインジケータは次のとおりです。

ブルートフォースアタック

認証試行の失敗を報告するsyslogメッセージ%ASA-6-113015の高いレートが表示される場合は、総当たり攻撃またはパスワードスプレー攻撃を示している可能性があります。総当たり攻撃では、通常、同じユーザおよび同じIPアドレスからこれらのメッセージが高い割合で発生します。パスワードスプレー攻撃では、同じIPアドレスを持つ一連のユーザに対して、通常これらのメッセージが高い割合で発生します。

次の例は、ユーザadminがIPアドレス172.16.17.18からの認証要求を使用して正常に認証できなかったことを示しています。

```
<#root>

%ASA-6-113015

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

user

 = admin : user

IP

 = 172.16.17.18
```

不正なクライアントレスSSL VPNセッションの確立

次の予期しない接続プロファイルまたはトンネルグループの1つを報告するセッション確立の試み(syslogメッセージ%ASA-7-734003)または終了イベント(syslogメッセージ%ASA-4-113019)が発生する場合、不正なクライアントレスSSL VPNセッションの確立が成功したか、または試行したことを示している可能性があります。

- DefaultADMINGroup
- DefaultL2LGroup

次の例は、ユーザadminが接続プロファイル/トンネルグループDefaultADMINGroupを使用して正常に認証されたセッションの確立を示しています。

```
<#root>

%ASA-7-734003

: DAP:

User

 admin, Addr 172.16.17.18: Session Attribute

aaa.cisco.tunnelgroup

 = DefaultADMINGroup
```

次の例は、接続プロファイル/トンネルグループDefaultADMINGroupを使用してユーザadminによって作成されたセッションが終了されたことを示しています。

```
<#root>

%ASA-4-113019

:

Group

 = DefaultADMINGroup,

Username

 = admin, IP = 172.16.17.18, Session disconnected. Session Type: SSL, Duration: 0h:00m:11s, Bytes xmt:
```

回避策

総当たり攻撃の試みを完全に防ぐ方法はありませんが、DefaultADMINGroupまたはDefaultL2LGroup接続プロファイル/トンネルグループを使用して、総当たり攻撃の影響を制限し、不正なクライアントレスSSL VPNセッションの確立を防ぐために、次の推奨事項を実装できます。

総当たり攻撃

ローカルユーザデータベースに対する総当たり攻撃

LOCALユーザデータベースに対する総当たり攻撃に対処するには、グローバルコンフィギュレーションモードでaaa local authentication attempts max-fail numberコマンドを使用して、ASAがLOCALユーザデータベース内の特定のユーザに許可する、連続して失敗するログイン試行の数を制限します。

ユーザが誤ったパスワードを使用して連続してログイン試行を設定回数だけ行うと、ユーザはロックアウトされ、管理者がclear aaa local user lockout username usernameコマンドを使用して手動でユーザのロックを解除するか（Cisco ASAソフトウェアリリース9.17以降を実行している場合）、10分経過するまで正常にログインできません。ユーザ名をロックまたはロック解除すると、次の例のようにsyslogメッセージが表示されます。

```
%ASA-6-113006: User 'test' locked out on exceeding '5' successive failed authentication attempts
%ASA-6-113007: User 'test' unlocked by 'enable_15'
```

注：Cisco ASAソフトウェアリリース9.16以前では、この機能は特権レベル15のユーザには適用されません。

この機能の詳細については、『Cisco Secure Firewall ASAシリーズコマンドリファレンス』を参照してください。

外部ユーザデータベースに対する総当たり攻撃

外部ユーザデータベースに対する総当たり攻撃に対処するには、外部ユーザデータベース内のユーザごとのログイン試行の連続失敗回数を制限します。

外部ユーザデータベースがCisco Identity Services Engine(ISE)の場合、これはAdministration > Identity Management > Settings > User Authentication Settings > Lock/Suspend Account with Incorrect Login Attemptsで設定できます。

注：外部ユーザデータベースに対する総当たり攻撃は、HTTPS管理認証、または少なくとも1つの接続プロファイル/トンネルグループが外部ユーザデータベースを指している場合にのみ可能です。

不正なクライアントレスSSL VPNセッションの確立

ダイナミックアクセスポリシー

管理者は、DefaultADMINGroupまたはDefaultL2LGroup接続プロファイル/トンネルグループが使用されている場合に、VPNトンネルの確立を終了するようにダイナミックアクセスポリシー

(DAP)を設定できます。DAPの設定方法の詳細については、『Cisco ASAシリーズVPN ASDMコンフィギュレーションガイド』の「ダイナミックアクセスポリシーの設定」セクションを参照してください。

デフォルトのグループポリシー(DfltGrpPolicy)を使用したリモートアクセスVPNの拒否

DfltGrpPolicyをリモートアクセスVPNポリシー割り当てに使用しない場合、管理者は次の例に示すようにDfltGrpPolicyのvpn-simultaneous-loginsオプションをゼロに設定することで、DefaultADMINGroupまたはDefaultL2LGroup接続プロファイル/トンネルグループを使用して、リモートアクセスVPNセッション確立を防止できます。

```
<#root>

group-policy DfltGrpPolicy attributes



vpn-simultaneous-logins 0
```

注：

- デフォルトでは、接続プロファイル/トンネルグループはDfltGrpPolicyを指しています。この回避策を適用する前に、管理者はtunnel-group name general-attributes設定モードでdefault-group-policyオプションを使用して、環境内のリモートアクセスVPNセッションの確立に使用されることが予期されるすべての接続プロファイルまたはトンネルグループがカスタムグループポリシーを指していることを確認する必要があります。特定の接続プロファイルまたはトンネルグループの実行コンフィギュレーションにdefault-group-policyオプションが表示されていない場合、その接続プロファイルまたはトンネルグループではDfltGrpPolicyが使用されます。
- デフォルトでは、カスタムグループポリシーはDfltGrpPolicyからvpn-simultaneous-logins設定を継承します。この回避策を適用する前に、管理者はリモートアクセスVPNセッションで使用されることが予想されるすべてのグループポリシーで、vpn-simultaneous-loginsオプションが0より大きい値に明示的に設定されていることを確認する必要があります。

ローカルユーザデータベース内のユーザの制限

次の2つの回避策は、HTTPS管理認証がLOCALユーザデータベースを指している場合にのみ、DefaultADMINGroupを使用するクライアントレスSSL VPNセッションの確立に適用されます。これらは常に、DefaultL2LGroupを使用するクライアントレスSSL VPNセッションの確立に適用されます。

特定の接続プロファイル/トンネルグループだけにユーザをロックする

LOCALユーザデータベース内のユーザがリモートアクセスVPNトンネルを確立できることが期待される場合、管理者はユーザ名属性設定モードでgroup-lockオプションを使用して、ユーザが特定の接続プロファイルまたはトンネルグループにのみ接続できるようにロックを設定できます。次の例は、ユーザlockeduserを接続プロファイル/トンネルグループMyCorporateProfileにロックする方法を示しています。

```
<#root>

username
 lockeduser
attributes


group-lock value
 MyCorporateProfile
```

ユーザによるリモートアクセスVPNセッションの確立の禁止

LOCALユーザデータベース内のユーザがリモートアクセスVPNトンネルをまったく確立できない場合、管理者はユーザ名属性設定モードのvpn-simultaneous-loginsオプションをゼロに設定することで、これらのユーザがリモートアクセスVPNトンネルを正常に確立するのを防ぐことができます。次に例を示します。

```
<#root>

username
 novpn
attributes


vpn-simultaneous-logins 0
```

これらの回避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。

Cisco FTDソフトウェアのホットフィックス

シスコはこの脆弱性に対処するために、次のホットフィックスをリリースしました。ホットフィックスは、Cisco.comのSoftware Centerからダウンロードできます。

Cisco FTD ソフトウェア リリース	ホットフィックス名
7.0.6	Cisco_FTD_Hotfix_EI-7.0.6.1-3.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_EI-7.0.6.1-3.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_EI-7.0.6.1-3.sh.RE L.tar Cisco_FTD_SSP_Hotfix_EI-7.0.6.1-3.sh.RE L.tar
7.2.5	Cisco_FTD_Hotfix_BJ-7.2.5.1-1.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_BJ-7.2.5.1-1.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_BJ-7.2.5.1-1.sh.RE L.tar Cisco_FTD_SSP_FP3K_Hotfix_BJ-7.2.5.1-1.sh.RE L.tar Cisco_FTD_SSP_Hotfix_BJ-7.2.5.1-1.sh.RE L.tar

これらのホットフィックスのダウンロードとインストールの詳細については、『シスコFirepowerホットフィックスリリースノート』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

2023年8月、Cisco Product Security Incident Response Team(PSIRT)は、この脆弱性の不正利用が試みられていることを認識しました。修正済みのソフトウェアリリースにアップグレードして、この脆弱性が利用可能になった時点で修正を行い、その間に推奨される回避策のいずれかを適用することを強くお勧めします。

この脆弱性の不正利用が確認された事例については、シスコのブログ記事「Akira Ransomware Targeting VPNs without Multi-Factor Authentication」を参照してください。このブログ記事で説明されているように、組織はVPN実装でMFAを有効にすることで、ランサムウェア感染の可能性を含む不正アクセスのリスクを大幅に削減できます。

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。

シスコは、この脆弱性の不正利用の試みを報告していただいたRapid7に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.4	アドバイザリのステータスをFinalに更新。修正済みソフトウェアが入手可能であることを示すために要約を更新。DfltGrpPolicyでvpn-simultaneous-logins 0を使用する意味を明確化。Cisco FTDソフトウェアホットフィックスを追加。	ヘッダー、サマリー、回避策、修正済みリリース	Final	2023年10月11日
1.3	ソフトウェアチェッカーのリンクを更新。	修正済みソフトウェア	Interim	2023-9-29
1.2	どの攻撃シナリオにどの回避策が適用されるかを明確にした。	回避策	Interim	2023 年 9 月 27 日
1.1	ブルートフォースアタックの定義を更新。Cisco FTDソフトウェアリリース7.0以降でのLOCALユーザデータベースのサポートに関する情報を明確化。総当たり攻撃に対する回避策を追加。	「脆弱性のある製品」および「回避策」	Interim	2023 年 9 月 11 日
1.0	初回公開リリース	—	Interim	2023 年 9 月 6 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を対象としています。

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。