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 WebVPN におけるサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20190501-sd-cpu-dos
CVE-2018-15388
初公開日 : 2019-05-01 16:00
最終更新日 : 2019-05-02 17:57
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvj33780

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 WebVPN ログイン プロセスの脆弱性により、認証されていないリモートの攻撃者が該当デバイスの CPU 使用率を上昇させることができる危険性があります。

この脆弱性は、既存の WebVPN ログイン操作で処理の負荷が過剰になることに起因します。攻撃者は、複数の WebVPN ログイン要求をデバイスに送信することにより、この脆弱性をエクスプロイトする危険性があります。エクスプロイトが成功すると、攻撃者がデバイスの CPU の負荷を増大させ、サービス妨害（DoS）状態が発生する危険性があります。

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-20190501-sd-cpu-dos

該当製品

脆弱性のある製品

WebVPN を設定している場合、この脆弱性は Cisco ASA ソフトウェアまたは FTD ソフトウェアを実行する次のシスコ製品に影響を与えます。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- 適応型セキュリティ アプライアンス（ASA）1000V クラウド ファイアウォール
- ASA 5505 シリーズ適応型セキュリティ アプライアンス[1]
- ASA 5500-X シリーズ ファイアウォール
- Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の ASA サービス モジュール
- 適応型セキュリティ仮想アプライアンス（ASAv）
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- FirePOWER 9300 ASA セキュリティ モジュール
- Firepower Threat Defense Virtual

1 ASA 5505 以外の ASA 5500 シリーズ適応型セキュリティ アプライアンスはサポートを終了したため、今後セキュリティ脆弱性に関する評価は行われません。

脆弱性が存在する Cisco ASA ソフトウェアおよび FTD 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。

WebVPN が有効になっているかどうかの確認

管理者が show running-config webvpn 特権 EXEC コマンドを使用してその出力を参照することにより、デバイスで WebVPN サービスが有効になっているかどうかを確認できます。次の例は、WebVPN サービスが有効になっているデバイスでのコマンドの出力を示しています。

<#root>

```
ciscoasa#
show running-config webvpn
```

```
.
.
.
webvpn
enable interface_name
.
.
.
```

Cisco ASA ソフトウェア リリースの判別

デバイス上で実行されている Cisco ASA ソフトウェア リリースは、管理者がデバイスにログインして CLI で show version | include Versionコマンドを使用して、コマンドの出力を参照します。デバイスが Cisco ASA ソフトウェア リリース 9.9.2.18 を実行している場合、コマンドの出力は次の例のようになります。

```
<#root>

ciscoasa#

show version | include Version

Cisco Adaptive Security Appliance Software Version 9.9.2.18
Device Manager Version 7.4(1)
.
.
.
```

デバイスが Cisco Adaptive Security Device Manager（ASDM）を使用して管理されている場合、管理者は Cisco ASDM ログイン ウィンドウまたは [Cisco ASDM ホーム（Cisco ASDM Home）] ペインの [デバイス ダッシュボード（Device Dashboard）] タブに表示される表のリリース情報を参照して、デバイスで実行中のリリースを確認することもできます。

Cisco FTD ソフトウェア リリースの判別

デバイスで実行中の Cisco FTD ソフトウェア リリースを確認するために、管理者はデバイスにログインし、CLI で show version コマンドを使用してコマンドの出力を参照できます。デバイスが Cisco FTD ソフトウェア リリース 6.2.0 を実行している場合、コマンドの出力例は次のようになります。

```
<#root>

>

show version


----------------------[ ftd ]----------------------
Model : Cisco ASA5525-X Threat Defense (75) Version 6.2.0 (Build 362)
UUID : 2849ba3c-ecb8-11e6-98ca-b9fc2975893c
Rules update version : 2017-03-15-001-vrt
VDB version : 279
---------------------------------------------------
```

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。

セキュリティ侵害の痕跡

この脆弱性がエクスプロイトされているときに、管理者が Unicorn プロキシ スレッド プロセスで CPU 使用率が上昇していることに気づく場合があります。これを確かめるには、CLI で show processes cpu-usage non-zero コマンドを発行し、Unicorn プロキシ スレッド プロセスの統計を確認します。

<#root>

```
ciscoasa# show processes cpu-usage non-zero
Hardware: ASA5516
Cisco Adaptive Security Appliance Software Version 9.8(2)38
ASLR enabled, text region 7f313ea71000-7f3142d61bb4
PC Thread 5Sec 1Min 5Min Process

0x00007f3140f35888   0x00002aaacfaa8b20     7.7%     5.0%     3.0%   Unicorn Proxy Thread


   -          -          9.5%     1.9%     0.8%   DATAPATH-0-2044
   -          -          3.6%     1.4%     0.8%   DATAPATH-1-2045
```

この出力の例は、上記のとおりです。管理者は、使用するデバイスの出力値と通常のデバイス動作の基準値を比較する必要があります。

回避策

この脆弱性に対処する回避策はありません。

エクスプロイトの実行中に、管理者が ACL を実装して着信要求をブロックするかレート制限を行うことにより、攻撃を軽減できる可能性があります。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通

常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] 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完全なアップグレード ソリューション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。

サービス契約をご利用でないお客様

シスコから直接購入したが Cisco Service Contract をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。本アドバイザリは以下のアドバイザリを含むコレクションの一部です。お客様におかれましては、これらも考慮したうえでアップグレード ソリューション全体をご確認ください。

- cisco-sa-20190501-asa-csrf:Cisco適応型セキュリティアプライアンスソフトウェアのクロスサイトリクエストフォージェリの脆弱性
- cisco-sa-20190501-asa-frpwrtd-dos: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Cisco Firepower Threat DefenseソフトウェアのTCPタイマー処理におけるDoS脆弱性
- cisco-sa-20190501-asa-ftd-dos: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(FTD)ソフトウェアのWebVPNにおけるDoS脆弱性
- cisco-sa-20190501-asa-ftd-entropy: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(FTD)ソフトウェアの低エントロピーキーの脆弱性
- cisco-sa-20190501-asa-ftd-ike-dos: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Cisco Firepower Threat Defense(FTD)ソフトウェアのMOBIKEにおけるサービス妨害の脆弱性

- cisco-sa-20190501-asaftd-saml-vpn:Cisco Adaptive Security Appliance(ASA)ソフトウェアおよびFirepower Threat Defense(FTD)ソフトウェアのVPNにおけるSAML認証バイパスの脆弱性
- cisco-sa-20190501-asa-ipsec-dos:Cisco適応型セキュリティアプライアンスソフトウェアのIPsecにおけるDoS脆弱性
- cisco-sa-20190501-firepower-dos:Cisco Firepower Threat DefenseソフトウェアのTCP入力ハンドラにおけるDoS脆弱性
- cisco-sa-20190501-frpwr-dos:Cisco Firepower Threat Defenseソフトウェアのパケット処理におけるDoS脆弱性
- cisco-sa-20190501-frpwr-smb-snort:Cisco Firepower Threat DefenseソフトウェアのSMBプロトコルプリプロセッサ検出エンジンにおけるDoS脆弱性
- cisco-sa-20190501-sd-cpu-dos: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(FTD)ソフトウェアのWebVPNにおけるサービス妨害の脆弱性

次の表では、左の列にシスコソフトウェアのリリースを記載しています。中央の列には、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。右の列は、リリースがこのアドバイザリ集に記載された何らかの脆弱性に該当するかどうか、および、それらすべての脆弱性に対する修正を含む最初のリリースを示しています。

Cisco ASA ソフトウェア

Cisco ASA ソフトウェア リリース	この脆弱性のための推奨リリース	このアドバイザリ集で説明している脆弱性すべてに対する推奨リリース
9.4 より前[1]	9.4.4.34	9.4.4.34
9.4	9.4.4.34	9.4.4.34
9.51	9.6.4.25	9.6.4.25
9.6	9.6.4.25	9.6.4.25
9.7	9.8.4	9.8.4
9.8	9.8.4	9.8.4
9.9	9.9.2.50	9.9.2.50
9.10	脆弱性なし	9.10.1.17
9.12	脆弱性なし	脆弱性なし

1 Cisco ASA ソフトウェアの 9.4 より前のリリース、Cisco ASA ソフトウェア リリース 9.5、および 9.7 については、メンテナンスが終了しています。この脆弱性に対する修正を含むサポート対象リリースに移行することをお勧めします。

Cisco FTD ソフトウェア

Cisco Firepower および FMC ソフトウェア	この脆弱性のための推奨リリース	このアドバイザリ集で説明している脆弱性すべてに対する推奨リリース
6.0	6.2.3.12	6.2.3.12
6.0.1	6.2.3.12	6.2.3.12
6.1.0	6.2.3.12	6.2.3.12
6.2.0	6.2.3.12	6.2.3.12
6.2.1	6.2.3.12	6.2.3.12
6.2.2	6.2.3.12	6.2.3.12
6.2.3	6.2.3.12	6.2.3.12
6.3.0	脆弱性なし	6.3.0.3
6.4.0	脆弱性なし	脆弱性なし

Cisco FTD ソフトウェアの修正済みリリースにアップグレードするには、次のいずれかの操作を行います。

- Cisco Firepower Management Center（FMC）を使用して管理しているデバイスについては、FMC インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。
- Cisco Firepower Device Manager（FDM）を使用して管理しているデバイスについては、FDM インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。

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

この脆弱性を報告していただいた Pratum 社の Jason Moulder 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-sd-cpu-dos

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	FTD ソフトウェア リリース 6.3.0.3 が使用可能になったことを示すために FTD の修正済みリリースの表を更新。	修正済みソフトウェア	Final	2019 年 5 月 2 日
1.0	初回公開リリース	-	Final	2019 年 5 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。