Cisco適応型セキュリティアプライアンスソフトウェアのVPNにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-20190501-asa-vpn-dos
CVE-2019-1705
初公開日 : 2019-05-01 16:00
最終更新日 : 2019-05-01 16:12
バージョン 1.1 : Final
CVSSスコア : 5.3
回避策 : Yes
Cisco バグ ID : CSCvk13637

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)ソフトウェアのリモートアクセスVPNセッションマネージャ(RDP)の脆弱性により、認証されていないリモートの攻撃者がリモートアクセスVPNサービスにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、リモートアクセスVPNセッションマネージャの問題に起因します。攻撃者は、過剰な数のリモートアクセスVPNセッションを要求することで、この脆弱性を不正利用する可能性があります。攻撃者はエクスプロイトにより、DoS 状態を引き起こす可能性があります。

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。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-20190501-asa-vpn-dos

該当製品

脆弱性のある製品

この脆弱性は、Cisco ASAソフトウェアに影響します。該当するソフトウェアリリースの詳細については、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。

次のシスコ製品は、マルチコンテキスト用に設定されている場合、この脆弱性の影響を受けます。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- 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
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス

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、その出力を参照することで確認できます。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 ASA設定の確認

ASAがマルチコンテキストモードで設定されているかどうかを確認するには、管理者がshow contextコマンドを使用します。次の表示は、show contextコマンドの出力例で、3つのコンテキストを示しています。

```
<#root>

hostname#

show context
```

```
Context Name      Interfaces                  URL

*admin            GigabitEthernet0/1.100      disk0:/admin.cfg

                  GigabitEthernet0/1.101

contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg

                  GigabitEthernet0/1.201

contextb          GigabitEthernet0/1.300      disk0:/contextb.cfg

                  GigabitEthernet0/1.301

Total active Security Contexts: 3
```

管理者は、show running-configコマンドを使用してASAでリモートアクセスVPNが設定されているかどうかを確認し、tunnel-group <tunnel_group_name> type remote-accessコマンドをチェックできます。

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。

詳細

この状態は、ユーザが最初のユーザ名/パスワード認証の後でPINまたは新しいパスワードの入力を求められたときに、ユーザがこの5分以内にこの情報を提供しなかった場合に発生します。この

間、ASAはプラットフォームによって定義されたプールから一時ライセンスを割り当てます。タイムアウト時間が経過すると、ASAはセッションの一時ライセンスの削除に失敗します。すべての一時ライセンスが割り当てられると、追加の接続は許可されません。

回避策

該当するデバイスで次のコマンドを使用すると、一時的に状態をクリアしたり、デバイスをリブートしたりできます。

```
vpn-sessiondb logoff all
```

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 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載の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。

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シスコのサービス契約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購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

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。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。右の列は、リリースがこのアドバイザリに記載された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。

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
9.4 より前[1]	脆弱性なし
9.4	9.4.4.34
9.51	9.6.4.25
9.6	9.6.4.25
9.7[1]	9.8.4
9.8	9.8.4
9.9	9.9.2.50
9.10	9.10.1.17
9.12	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。

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-20190501-asa-vpn-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	「Cisco FTDソフトウェアリリースと修正済みリリースの判別」でFirepower Threat Defense(FTD)ソフトウェアの参照を削除。	Cisco FTDソフトウェアリリースと修正済みリリースの判別	Final	2019 年 5 月 1 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。