Cisco適応型セキュリティアプライアンスソフトウェアのSSHサーバリソースにおけるDenial of Service(DoS)の脆弱性

Medium

アドバイザリーID : cisco-sa-asa-ssh-dos-eEDWu5RM
CVE-2024-20526
初公開日 : 2024-10-23 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : Yes
Cisco バグ ID : CSCwm49153

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SSHサーバにおける脆弱性により、認証されていないリモートの攻撃者が、該当デバイスのSSHサーバにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、SSHセッションの確立時に発生する論理エラーが原因です。攻撃者は、巧妙に細工されたSSHメッセージを該当デバイスに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。エクスプロイトに成功すると、攻撃者は該当デバイスで利用可能なSSHリソースを枯渇させ、デバイスへの新しいSSH接続を拒否して、DoS状態を引き起こす可能性があります。デバイスへの既存のSSH接続は、引き続き正常に機能します。回復するには、デバイスを手動で再起動する必要があります。ただし、ユーザトラフィックは影響を受けず、Cisco Adaptive Security Device Manager(ASDM)などのリモートアプリケーションを使用して管理できます。

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-asa-ssh-dos-eEDWu5RM

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ソフトウェアリリース9.16.4.67、9.16.4.70、9.18.4.40、または9.20.3を実行しているデバイスでSSHが有効になっており、独自のASA SSHスタックを使用するように設定されている場合に、これらのデバイス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。

デバイス設定の確認

SSHサーバはデフォルトでは有効になっていません。SSHサーバは、管理者がssh { ip_address mask | ipv6_address/prefix } interfaceコマンドを使用して取得できます。

Cisco ASAソフトウェアリリース9.16.4.67または9.16.4.70を実行していて、SSHが有効になっているデバイスは、この脆弱性の影響を受けます。デバイスがCisco ASAソフトウェアリリース9.18.4.40または9.20.3を実行している場合、次の例に示すように、show running-configコマンドがno ssh stack ciscosshを返す場合にのみ、この脆弱性の影響を受けます。

<#root>

```
asa#

show running-config ssh | include stack
no ssh stack ciscossh
```

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 Threat Defense（FTD）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

Cisco ASAソフトウェアでは、コンテキストごとに最大5つの同時SSH接続が可能です。この制限に達すると、これ以上の接続は許可されません。デバイス上で現在有効なSSHセッションの数を判断するには、show resource usageコマンドを使用して、SSH Serverの行を調べます。次の例に示すように、現在の数値が上限を1つ上回り、これが一定の期間にわたり明瞭にならない場合、そのデバイスは脆弱性によって不正利用された可能性があります。

```
<#root>

asa#

show resource usage

Resource                Current         Peak      Limit        Denied Context

SSH Server                    6            6          5             0 System


ASDM                          0            4         30             0 System
Syslogs [rate]               18         1536        N/A             0 System
Conns                      8547        32540     500000             0 System
```

この状態をクリアするには、デバイスを手動でリブートする必要があります。管理者は別のコンテキストでSSHを使用したり、コンソールポートにアクセスしたりできますが、これは常に可能とは限りません。

回避策

Cisco ASAソフトウェアリリース9.16.4.67または9.16.4.70を実行しているデバイスでは、この脆弱性に対する回避策はありません。

Cisco ASAソフトウェアリリース9.18.4.40または9.20.3を実行しているデバイスの場合は、ssh stack ciscossh CLIコマンドを使用して、CiscoSSHスタックを使用するようにデバイスを設定します。この脆弱性の影響を受けません。このコマンドの実装の詳細については、『Cisco Secure Firewall ASAシリーズコマンドリファレンス』の「ssh stack ciscossh」セクションを参照してください。

こ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	

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。

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

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-asa-ssh-dos-eEDWu5RM

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。