Cisco Secure Firewall適応型セキュリティアプライアンスソフトウェアのSSHの部分的な秘密キー認証バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-asa-ssh-keybypass-cr5xPUSf
初公開日 : 2026-03-04 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCwq24081

CVE-2026-20009

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 Secure Firewall適応型セキュリティアプライアンス(ASA)ソフトウェアにおける、SSHキーベースの認証を使用した独自のSSHスタックの実装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Cisco Secure Firewall ASAデバイスにログインし、特定のユーザとしてコマンドを実行できる可能性があります。

この脆弱性は、SSH認証フェーズでのユーザ入力の検証が不十分であることに起因します。攻撃者は、SSH認証中に巧妙に細工された入力を該当デバイスに送信することで、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、特定のユーザのプライベートSSHキーを使用せずに、そのユーザとしてデバイスにログインできる可能性があります。この脆弱性を不正利用するには、攻撃者が有効なユーザ名と関連する公開キーを所有している必要があります。秘密キーは必要ありません。

注：

- この脆弱性の不正利用によって攻撃者がルートアクセスを取得することはありません。
- 認証、認可、アカウンティング(AAA)コンフィギュレーションコマンドauto-enableは、この脆弱性の影響を受けません。

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-asa-ssh-

keybypass-cr5xPUSf

このアドバイザリは、2026年3月に公開された『Cisco Secure Firewall ASA、Secure FMC、およびSecure 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。アドバイザリとリンクの一覧については、『Cisco Event Response: March 2026 Semiannual Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

この脆弱性の公開時点では、Cisco Secure Firewall ASAソフトウェアの脆弱性が存在するリリースを実行するシスコ製品に影響が及び、次の条件が満たされていました。

- Cisco SSHスタックを有効にしました。Cisco SSHスタックは、Cisco Secure Firewall ASAソフトウェアリリース9.17.1で初めて導入されました。
- デバイスはSSHキーベースの認証用に設定されています。
- 少なくとも1つのインターフェイスでSSHアクセスが許可されました。

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。

Cisco SSHスタックが有効になっているかどうかの確認

デバイスでCiscoSSHスタックが有効になっているかどうかを確認するには、show running-config | include sshコマンドを使用します。次の例に示すように、ssh stack ciscossh設定とSSH ACLが存在することを確認します。

```
<#root>

ciscoasa#

show running-config | include ssh


aaa authentication ssh console LOCAL
ssh scopy enable

ssh stack ciscossh


ssh stricthostkeycheck
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group14-sha256


ssh

0.0.0.0 0.0.0.0 management
```

```
ciscoasa#
```

上記の例では、SSH には管理インターフェイスを介してのみアクセスできます。出力にssh stack ciscosshが含まれていない場合、そのデバイスはこの脆弱性の影響を受けません。

SSHキーベース認証が有効になっているかどうかの確認

デバイスでSSHキーベースの認証が有効になっているかどうかを確認するには、show running-config | include sshコマンドを使用します。次の例に示すように、ssh authentication publickey設定が存在することを確認します。

<#root>

```
ciscoasa#
show run | include ssh


aaa authentication ssh console LOCAL
ssh scopy enable
ssh stack ciscossh
ssh stricthostkeycheck
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group14-sha256


ssh 0.0.0.0 0.0.0.0 management
ssh authentication publickey
 ...


ciscoasa#
```

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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。

- Cisco Secure Firewall Threat Defense（FTD）ソフトウェア
- Cisco Secure Firewall Management Center（FMC）ソフトウェア

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェア

お客様が Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアにおける脆弱性のリスクの有無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、セキュリティへの影響の評価（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 Secure Firewall ASA ソフトウェアの場合は 9.20.3.4、Cisco Secure FTD ソフトウェアの場合は 7.4.2 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	

関連情報

最適な Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各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 Secure Firewall 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、内部セキュリティテストで Cisco Advanced Security Initiatives Group（ASIG）の T.VE によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-keybypass-cr5xPUSf

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	2026年3月4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。