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マルチコンテキストモードSCPの不正なファイルアクセスの脆弱性

High

アドバイザリーID : cisco-sa-asa-scpcxt-filecpy-rgeP73nE
初公開日 : 2026-03-04 16:00
バージョン 1.0 : Final
CVSSスコア : 7.2
回避策 : No workarounds available
Cisco バグ ID : CSCwp05866

CVE-2026-20062

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

マルチコンテキストモードのCisco Secure Firewall適応型セキュリティアプライアンス(ASA)ソフトウェアのCLIにおける脆弱性により、あるコンテキストで管理者権限を持つ認証されたローカルの攻撃者が、コンフィギュレーションファイルを含む別のコンテキストとの間でファイルをコピーできるようになります。

この脆弱性は、Cisco SSHスタックが有効な場合のSecure Copy Protocol(SCP)操作のアクセスコントロールが不適切なことに起因します。攻撃者は、デバイスの非管理コンテキストに対して認証を行い、その非管理コンテキストで巧妙に細工されたSCP copyコマンドを発行することにより、この脆弱性をエクスプロイト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、管理コンテキストやシステムコンテキストなど、別のコンテキストに属する機密ファイルを読み取り、作成、または上書きできるようになります。攻撃者は、他のコンテキストに関連するサービスの可用性に直接影響を与えることはできません。この脆弱性を不正利用するには、攻撃者は非管理コンテキストに対する有効な管理クレデンシャルを持っている必要があります。

注：攻撃者は別のコンテキストからファイルをリストまたは列挙できないため、正確なファイルパスを知る必要があり、成功する攻撃の複雑さが増します。

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-scpcxt-filecpy-rgeP73nE

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

この脆弱性は、Cisco Secure Firewall ASAソフトウェアの脆弱性のあるリリースを実行し、次の両方の条件を満たすシスコ製品に影響を与えます。

- マルチコンテキストモードが設定されている。
- Cisco SSHスタックが有効になっている。

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。

マルチコンテキストモードが有効になっているかどうかを確認する

マルチコンテキストモードが有効になっているかどうかを確認するには、show modeコマンドを使用します。そのコマンドの出力に、次の例に示すようにmultipleと表示される場合は、マルチコンテキストモードが有効になっています。

```
<#root>

ciscoasa#

show mode

Security context mode:

multiple

ciscoasa#
```

出力にsingleと示されている場合、マルチコンテキストモードは有効ではなく、デバイスは脆弱ではないと考えられます。

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Cisco SSHスタックが有効になっているかどうかを確認するには、次の例に示すように、show ssh | include stackコマンドを使用してciscoSSH stackが有効になっているかどうかを確認します。

```
<#root>

ciscoasa#

show ssh | include stack


ciscoSSH stack  : ENABLED


ciscoasa#
```

出力が空であるか、ciscoSSHスタックがDISABLEDと報告された場合、Cisco SSHスタックは有効ではなく、デバイスに脆弱性があるとは見なされません。

注：

- 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。
- Cisco Secure Firewall ASAソフトウェアリリース9.23.1以降でサポートされているSSHスタックはCisco SSHのみです。

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

エア

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 Cisco Cisco Technical Assistance Center（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-scpcxt-filecpy-rgeP73nE

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。