Firepower 1000、2100、3100、4200シリーズ向けCisco Firepower Threat Defenseソフトウェアの静的クレデンシャルの脆弱性

アドバイザリーID : cisco-sa-ftd-statcred-dFC8tXT5
CVE-2024-20412
初公開日 : 2024-10-23 16:00
バージョン 1.0 : Final
CVSSスコア : 9.3
回避策 : Yes
Cisco バグ ID : CSCwk07982

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 Firepower 1000、2100、3100、および4200シリーズ用のCisco Firepower Threat Defense(FTD)ソフトウェアの脆弱性により、認証されていないローカルの攻撃者が静的クレデンシャルを使用して該当システムにアクセスする可能性があります。

この脆弱性は、影響を受けるシステムに、ハードコードされたパスワードを持つ静的アカウントが存在することに起因します。攻撃者は、これらのクレデンシャルを使用して該当デバイスのCLIにログインすることにより、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、攻撃者は該当システムにアクセスして機密情報を取得したり、限定されたトラブルシューティング操作を実行したり、一部の設定オプションを変更したり、デバイスをオペレーティングシステムから起動できなくしたりすることが可能になり、デバイスの再イメージ化が必要になります。

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-ftd-statcred-dFC8tXT5

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

この脆弱性は、387以前のVulnerability Database(VDB)リリースでCisco FTDソフトウェアリリース7.1 ~ 7.4を実行する次のシスコ製品に影響を与える可能性があります。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firepower 3100 シリーズ
- Firepower 4200 シリーズ

注：リリース7.1よりも前のCisco FTDソフトウェアリリースからリリース7.1以降にアップグレードされたデバイスは該当しません。

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。

静的アカウントが存在するかどうかを確認する

デバイスに特定の静的アカウントが存在するかどうかを確認するには、Cisco FXOS CLIのsecurityスコープでshow local-userコマンドを使用します。次のshow local-userの出力は、特定の静的アカウントの存在を示しています。

<#root>

```
Firepower#
scope security
Firepower /security #
 show local-user

User Name       First Name      Last name
--------------- --------------- ---------
.
.
.
csm_processes


report


sftop10user
```

```
Sourcefire


SRU
.
.
.

Firepower /security #
```

脆弱性を含んでいないことが確認された製品

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。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- FTDソフトウェアが次のプラットフォームで実行されている場合：
  - ASA 5500-X シリーズ
  - Firepower 4100 シリーズ
  - Firepower 9300 シリーズ
  - セキュアファイアウォールISA3000
- Secure Firewall Management Center(FMC)ソフトウェア（旧称：Firepower Management Center Software）
- Secure Firewall Threat Defense Virtual（旧称FTDv/NGFWv）

詳細

Cisco FTDソフトウェアを実行しているデバイスのCLIにアクセスするには、2つの方法があります。1つ目は、リモートアクセス用にターミナルサーバに接続できる物理シリアルポートを使用する方法です。2つ目はSSHを使用する方法です。SSHはデバイスの管理インターフェイスでデフォルトで有効になっています。SSHは、データインターフェイスでも有効にできます。データインターフェイスでSSHが有効になっているかどうかを確認するには、CLIでshow running-config sshコマンドを使用します。次の出力は、外部インターフェイスでSSHが有効になっていることを示しています。

```
<#root>

>

show running-config ssh


ssh 10.1.2.0 255.255.255.0 outside
>
```

注：show running-config sshコマンドの出力がない場合、SSHは管理インターフェイスでのみ有効になっています。

SSHアクセスはアクセスコントロールリスト(ACL)によって制限できますが、これにより攻撃対象領域が縮小されるだけで、脆弱性は緩和されません。

デバイスへの管理アクセスの設定の詳細については、次のマニュアルを参照してください。

- Cisco Firepower Device Manager(FDM)の場合：管理アクセスの設定
- Cisco FMCソフトウェアの場合、SSHアクセス

セキュリティ侵害の痕跡

デバイスで最近、静的アカウントへのアクセスが発生したかどうかを確認するには、expertモードでrootユーザとして、zgrep -E "Accepted password for (csm_processes|report|sftop10user|Sourcefire|SRU)" /ngfw/var/log/messages* コマンドを使用します。次の出力は、reportユーザが正常にアクセスしたことを示しています。

```
<#root>

>

expert


admin@intel-x86-6d:~$

sudo su root


admin@intel-x86-6d:~$

zgrep -E "Accepted password for (csm_processes|report|sftop10user|Sourcefire|SRU)" /ngfw/var/log/message


/ngfw/var/log/messages:Jun 17 16:55:56 intel-x86-6d sshd[48987]: Accepted password for

report

 from 10.1.2.3 port 56261 ssh2
admin@intel-x86-6d:~$
```

注：zgrep -E "Accepted password for (csm_processes|report|sftop10user|Sourcefire|SRU)" /ngfw/var/log/messages*コマンドは1行で入力する必要があります。

出力が返されない場合は、ログの保持期間中にデバイス上の脆弱なアカウントにアクセスしていません。保存期間を確認するには、/ngfw/var/log/messages*ファイルに関連する日付を確認します。

回避策

この脆弱性の回避策は、修整版リリースにアップグレードできないお客様に使用できます。回避策の実装の調整に関しては、 Cisco Technical Assistance Center (TAC) にお問い合わせください。

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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス (My Devices)] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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。

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。

Cisco FTD VDBアップデート

システムのリロードを必要とするベースソフトウェアアップグレードの適用を希望しない場合は、該当するデバイスにVDBリリース388以降をインストールできます。このVDBリリースにより、この脆弱性は解決されます。

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	

Cisco FTDデバイスのアップグレード手順については、該当する『Cisco FMC upgrade guide』を参照してください。

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-ftd-statcred-dFC8tXT5

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。