Cisco Secure Firewall Management Centerソフトウェアのスタティッククレデンシャルの脆弱性

アドバイザリーID : cisco-sa-fmc-static-cred-BET3Cjh
初公開日 : 2026-07-29 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 : CSCwt95997

CVE-2026-20316

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 Management Center(FMC)ソフトウェアのWebインターフェイス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、権限の低いアカウントを使用して該当デバイスにログインし、該当システム内の機密データにアクセスする可能性があります。

この脆弱性は、権限の低いアカウントに静的なユーザクレデンシャルが存在することに起因します。攻撃者は、そのアカウントを使用して該当システムにログインすることで、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、攻撃者は該当システムにログインし、権限の低いユーザとして機密データにアクセスできる可能性があります。

注：FMC 管理インターフェイスにパブリック インターネット アクセスがない場合、この脆弱性に関連する攻撃対象領域が小さくなります。

スコアに示されているように、シスコはこのセキュリティアドバイザリのセキュリティ影響評価（SIR）に Medium（中）ではなく High（高）を割り当てています。その理由は、この脆弱性を他のCisco Secure FMCソフトウェアの脆弱性と組み合わせて使用することで、権限を昇格できるためです。

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。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-fmc-static-cred-BET3Cjh

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、Cisco Secure FMC ソフトウェアに影響を与えます。

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。

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。

- クラウド提供型 FMC（cdFMC）
- ファイアウォールデバイスマネージャ(FDM)
- 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
- Cisco Secure Firewall Threat Defense（FTD）ソフトウェア
- Security Cloud Control（SCC）（旧 Defense Orchestrator）

セキュリティ侵害の痕跡

この脆弱性が不正利用された可能性があるかどうかを判断するには、expert モードでCLIコマンドcat /var/log/messages | grep license を使用します。次の例に示すように、出力のログメッセージに/var/tmp/license.tmpが含まれている場合、この脆弱性はCisco Secure FMCデバイスで不正利用されている可能性があります。

<#root>

expert

```
admin@firepower:~$ sudo su
Password:
Last login: Thu Jul 23 19:40:57 UTC 2026 on pts/2
root@firepower:/home/admin#
root@firepower:/home/admin#
```

cat /var/log/messages | grep license

```
Jul 23 16:16:33 firepower sudo:
```

www : PWD=/ ; USER=root ; COMMAND=/usr/local/sf/bin/package_info.pl /var/tmp/license.tmp

```
 --lsm
```

不正利用が疑われる場合は、Cisco Technical Assistance Center(TAC)に連絡して、回復オプションのサポートを依頼してください。シスコでは、この脆弱性のアクティブなエクスプロイトが進行中であるため、少なくとも、Cisco Secure FMCデバイス上のすべてのユーザクレデンシャル、キー、および証明書をローテーションすることを推奨します。

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 FMCホットフィックス

シスコは、この脆弱性に対処するために次のホットフィックスをリリースしました。これらのホットフィックスを Cisco.com の Software Center からダウンロードできます。

Cisco Secure FMCソフトウェアリリース	ホットフィックス名
7.0	Cisco_Firepower_Mgmt_Center_Hotfix_GB-7.0.9.1-3.sh.REL.tar
7.2	Cisco_Secure_FW_Mgmt_Center_Hotfix_HL-7.2.11.1-4.sh.REL.tar
7.4	Cisco_Secure_FW_Mgmt_Center_Hotfix_HG-7.4.7.1-3.sh.REL.tar
7.6	Cisco_Secure_FW_Mgmt_Center_Hotfix_CY-7.6.5.1-2.sh.REL.tar
7.7	Cisco_Secure_FW_Mgmt_Center_Hotfix_AM-7.7.12.1-2.sh.REL.tar
10.0	Cisco_Secure_FW_Mgmt_Center_Hotfix_P-10.0.1.1-2.sh.REL.tar

これらのホットフィックスのダウンロードとインストールの詳細については、『Cisco Firepowerホットフィックスリリースノート』を参照してください。

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデ

ント レスポンス チーム) は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

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

2026年7月、Cisco PSIRTはこの脆弱性が活発に悪用されていることを認識しました。この脆弱性が修正済みのソフトウェアリリースにアップグレードすることを強くお勧めします。

出典

シスコは、この脆弱性を報告していただいたHorizon3.aiのJimi Sebree氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh

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7月29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。