Cisco Firepower Management Centerのスタティッククレデンシャルの脆弱性

Medium

アドバイザリーID : cisco-sa-fmcua-statcred-weeCcZct
初公開日 : 2020-05-06 16:00
バージョン 1.0 : Final
CVSSスコア : 8.1
回避策 : No workarounds available
Cisco バグ ID : CSCvo08211 CSCvq50674

CVE-2020-3318
CVE-2020-3301

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 Management Center(FMC)ソフトウェアおよびCisco Firepower User Agentソフトウェアの複数の脆弱性により、攻撃者が高特権アカウントを使用して該当システムの機密部分にアクセスする可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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-fmcua-statcred-weeCcZct

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性は、リリース2.5.0より前のFirepowerユーザエージェントソフトウェアリリースが有効になっている場合、リリース6.5.0より前のCisco FMCソフトウェアリリースに影響を与えました。

注：この脆弱性は、Adaptive Security Device Manager(ASDM)で管理されているCisco適応型セキュリティアプライアンス(ASA)にも影響を与えます。ASAを管理するには、Cisco Firepower Servicesリリース6.5.0にアップグレードするか、Cisco FMCソフトウェアにアップ

グレードすることをお勧めします。

最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

Firepowerユーザエージェントが有効になっているかどうかの確認

Cisco Firepower User Agentが有効になっているかどうかを確認するには、Web UIで次の手順を実行します。

1. System > Integration > Identity Sourcesの順に選択します。
2. User Agentが選択されているかどうかを確認します。
3. どのIPアドレスがFMCへのアクセスを許可するように設定されているかを確認します。

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。

シスコでは、この脆弱性が Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアまたは Cisco Firepower Threat Defense（FTD）ソフトウェアに影響を及ぼさないことを確認しています。

詳細

Cisco FMCソフトウェアとCisco Firepower User Agentソフトウェアの2つの脆弱性により、攻撃者が高特権アカウントを使用してシステムの機密部分にアクセスする可能性があります。

脆弱性の詳細は以下のとおりです。

Cisco Firepower Management Centerのスタティッククレデンシャルの脆弱性

Cisco FMCソフトウェアの脆弱性により、認証されていないリモートの攻撃者が、高い権限を持つアカウントを使用して該当システムの機密部分にアクセスする可能性があります。

この脆弱性は、デフォルトの静的パスワードを持つシステムアカウントがシステム管理者によって制御されないことに起因します。このデフォルトアカウントで該当システムにログインされると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、攻撃者はユーザエージェントデータに対する読み取りおよび書き込みアクセス権を取得できる可能性があります。攻撃者はシステムの機密部分にアクセスできますが、デバイスを制御するための完全な管理者権限はありません。

バグID:CSCvq50674
CVE ID：CVE-2020-3318
セキュリティ影響評価（SIR）：中

CVSS ベーススコア：8.1
CVSSベクトル：CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Cisco Firepowerユーザエージェントのスタティッククレデンシャルの脆弱性

Cisco Firepower User Agentソフトウェアの脆弱性により、認証されたローカルの攻撃者が、特権の高いアカウントを使用して該当システムの機密部分にアクセスできる可能性があります。

この脆弱性は、システムアカウントにデフォルトの静的パスワードが設定されており、システム管理者によって制御されていないことに起因します。このデフォルトアカウントで該当システムにログインされると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、攻撃者はユーザエージェントデータに対する読み取りおよび書き込みアクセス権を取得できる可能性があります。攻撃者はシステムの機密部分にアクセスできますが、デバイスを制御するための完全な管理者権限はありません。

バグID:CSCvo08211
CVE ID：CVE-2020-3301
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：7.1
CVSSベクトル：CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] 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完全なアップグレード ソリューション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。

修正済みリリース

公開時点では、Cisco FMCソフトウェアリリース6.5.0以降およびFirepower User Agentソフトウェアリリース2.5.0以降にこれらの脆弱性に対する修正が含まれています。[1]。これらの脆弱性に対処するには、Cisco FMCソフトウェアとCisco Firepower User Agentソフトウェアの両方をアップグレードする必要があります。

注：ASDMで管理されているASAを使用しているお客様は、Cisco Firepower Servicesリリース6.5.0にアップグレードするか、Cisco FMCソフトウェアにアップグレードすることをお勧めします。

最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

1. Cisco FMC および FTD ソフトウェア リリース 6.0.1 以前については、メンテナンスが終了しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcua-statcred-weeCcZct

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	2020 年 5 月 6 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。