Cisco Secure Firewall Management Centerソフトウェアの SQLインジェクションの脆弱性

アドバイザリーID : cisco-sa-fmc-sql-injection-2qH6CcJd
初公開日 : 2026-03-04 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 : CSCwq01517 CSCwp22451 CSCwo65318

CVE-2026-20002
CVE-2026-20003
CVE-2026-20001

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ベースの管理インターフェイスとREST APIの複数の脆弱性により、認証されたリモートの攻撃者が該当システムでSQLインジェクション攻撃を実行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-fmc-sql-injection-2qH6CcJd

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

これらの脆弱性は、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」セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- 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

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2026-20002:Cisco Secure FMCソフトウェアのSQLインジェクションの脆弱性

Cisco Secure FMCソフトウェアのWebベースの管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、該当システムでSQLインジェクション攻撃を実行する可能性があります。

この脆弱性は、ユーザ入力の検証が不適切であることに起因します。攻撃者は、巧妙に細工された要求を該当デバイスに送信することにより、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、攻撃者はデータベースへのフルアクセス権を取得し、基盤となるオペレーティングシステム上の特定のファイルを読み取る可能性があります。この脆弱性を不正利用するには、攻撃者は有効なユーザクレデンシャルを必要とします。

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。この脆弱性に対処する回避策はありません。

バグID: CSCwq01517
CVE ID：CVE-2026-20002
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.1
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVE-2026-20001:Cisco Secure FMCソフトウェアのSQLインジェクションの脆弱性

Cisco Secure FMCソフトウェアのREST APIの脆弱性により、認証されたリモートの攻撃者が該当システムでSQLインジェクション攻撃を実行できる可能性があります。

この脆弱性は、ユーザ入力の検証が不適切であることに起因します。攻撃者は、巧妙に細工された要求を該当デバイスに送信することにより、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、攻撃者はデータベースへの読み取りアクセス権を取得し、基盤となるオペレーティングシステム上の特定のファイルを読み取る可能性があります。この脆弱性を不正利用するには、攻撃者は次のいずれかのロールを持つ有効なユーザクレデンシャルを必要とします。

- Administrator
- セキュリティ承認者
- 管理者へのアクセス
- ネットワーク管理者

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。

バグID: CSCwo65318
CVE ID：CVE-2026-20001
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.9
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVE-2026-20003:Cisco Secure FMCソフトウェアのSQLインジェクションの脆弱性

Cisco Secure FMCソフトウェアのREST APIの脆弱性により、認証されたリモートの攻撃者が該当システムでSQLインジェクション攻撃を実行できる可能性があります。

この脆弱性は、ユーザ入力の検証が不適切であることに起因します。攻撃者は、巧妙に細工された要求を該当デバイスに送信することにより、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、攻撃者はデータベースへの読み取りアクセス権を取得し、基盤となるオペレーティングシステム上の特定のファイルを読み取る可能性があります。この脆弱性を不正利用するには、攻撃者は次のいずれかのロールを持つ有効なユーザクレデンシャルを必要とします。

- Administrator
- セキュリティ承認者
- 侵入管理者
- 管理者へのアクセス
- ネットワーク管理者

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。

バグID: CSCwp22451
CVE ID：CVE-2026-20003
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.9
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

回避策

これら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。これら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）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

出典

CVE-2026-20002：この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のKyle Ossinger氏によって、内部セキュリティテスト中に発見されました。

CVE-2026-20001およびCVE-2026-20003：これらの脆弱性は、シスコの社内セキュリティテストでSanmith Prakash氏によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sql-injection-2qH6CcJd

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

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。