Cisco FXOSおよびUCS Managerソフトウェアのストアドクロスサイトスクリプティングの脆弱性

アドバイザリーID : cisco-sa-ucsfxosxss-7skVE8Zv
初公開日 : 2026-02-25 16:00
バージョン 1.0 : Final
CVSSスコア : 4.8
回避策 : No workarounds available
Cisco バグ ID : CSCwm83088 CSCwm83089 CSCwm57437

CVE-2026-20091

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 FXOSソフトウェアおよびCisco UCS Managerソフトウェアのwebベース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、そのインターフェイスのユーザに対して保存されたクロスサイトスクリプティング(XSS)攻撃を実行する可能性があります。

この脆弱性は、該当システムのWebベース管理インターフェイスでユーザ入力の検証が不十分なことに起因します。攻撃者は、悪意のあるデータをインターフェイスの特定のページに挿入することで、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、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスす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AdministratorまたはAAA Administratorのロールを持つユーザアカウントの有効なクレデンシャルを持っている必要があります。

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。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-ucsfxosxss-7skVE8Zv

このアドバイザリは、2026年2月に公開されたCisco FXOSおよびNX-OS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: February 2026 Semiannual Cisco FXOS and NX-OS 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

公開時点で、Cisco FXOSソフトウェアまたはUCS Managerソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品がこの脆弱性の影響を受けました。

- プラットフォームモードで動作するFirepower 2100シリーズ(CSCwm83088)
- Firepower 4100シリーズ(CSCwm83089)
- Firepower 9300セキュリティアプライアンス(CSCwm83089)
- UCS 6300シリーズファブリックインターコネクト(CSCwm57437)
- UCS 6400シリーズファブリックインターコネクト(CSCwm57437)
- UCS 6500シリーズファブリックインターコネクト(CSCwm57437)
- UCS Xシリーズダイレクトファブリックインターコネクト9108 100G(CSCwm57437)

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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。

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。

- Firepower 1000 シリーズ
- アプライアンスモードで動作するFirepower 2100シリーズ
- MDS 9000 シリーズ マルチレイヤ スイッチ
- Nexus 3000 シリーズ スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- ACI モードの Nexus 9000 シリーズ ファブリック スイッチ
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- Cisco Secure Firewall 200 シリーズ
- Cisco Secure Firewall 1200 シリーズ
- Cisco Secure Firewall 3100 シリーズ

- Cisco Secure Firewall 4200 シリーズ
- Cisco Secure Firewall 6100 シリーズ
- UCS 6600 シリーズ ファブリック インターコネクト

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 FXOS ソフトウェア

お客様がCisco FXOSソフトウェアの脆弱性による問題の可能性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。このアドバイザリのみ、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、すべてのアドバイザリのいずれかです。
2. 該当するプラットフォームを選択します。注：Firepower 2100シリーズアプライアンスは、Cisco ASAソフトウェアユニファイドイメージバンドルまたはCisco FTDソフトウェアユニファイドイメージバンドルに含まれているCisco FXOSソフトウェアを基盤オペレーティングシステムとして使用します。ASAまたはFTDソフトウェアを選択して、そのプラットフォームの結果を取得します。
3. リリース番号を入力します(例：Cisco Firepower 4100シリーズセキュリティアプライアンスの場合、2.14.1.131)。
4. [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 FXOS ソフトウェア	あらゆるプラットフォーム

Enter release number | Check

Cisco UCS ソフトウェア

発行時点では、次の表に示すリリース情報は正確でした。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。

左の列はシスコソフトウェアリリースを、右の列はリリースがこのアドバイザリに記載された脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

UCS 6300シリーズ、6400シリーズ、6500シリーズ、および9108 100Gファブリックインターコネクト

Cisco UCS ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
4.2 以前	修正済みリリースに移行。
4.3	4.3 (6a)
6.0	脆弱性なし

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。

不正利用事例と公式発表

Cisco PSIRT では、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とその公表は確認しておりません。

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-ucsfxosxss-7skVE8Zv

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2月25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。