

# Cisco Integrated Management Controllerの仮想キーボードビデオモニタオープンリダイレクトの脆弱性



アドバイザリーID : cisco-sa-ucs-vkvmorv- [CVE-2025-20317](#)  
CnKrV7HK

初公開日 : 2025-08-27 16:00

バージョン 1.0 : Final

CVSSスコア : [7.1](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwo04043](#) [CSCwn43942](#)

[CSCwm57436](#) [CSCwo77400](#)

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 Integrated Management Controller(IMC)の仮想キーボードビデオモニタ(vKVM)接続処理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悪意のあるWebサイトにユーザをリダイレクトする可能性があります。

この脆弱性は、vKVMエンドポイントの不十分な検証に起因します。攻撃者は、ユーザーを、巧妙に細工されたリンクをクリックするように誘導することで、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、攻撃者はユーザを悪意のあるWebページにリダイレクトし、ユーザクレデンシャルを取得できる可能性があります。

注 : 影響を受けるvKVMクライアントは、Cisco UCS Managerにも含まれています。

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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-vkvmorv-CnKrV7HK>

## 該当製品

脆弱性のある製品

この脆弱性は、デバイス設定に関係なく、脆弱性のあるソフトウェアリリースを実行している次のシスコ製品に影響を与えます。

- Catalyst 8300シリーズEdge uCPE([CSCwo77400](#))
- UCS Managerソフトウェア([CSCwo04043](#))
- UCS Bシリーズブレードサーバ([CSCwm57436](#))
- UCS CシリーズM6、M7、およびM8ラックサーバ([CSCwn43942](#))
- UCS EシリーズサーバM6([CSCwo77400](#))
- UCS Xシリーズモジュラシステム([CSCwm57436](#))

上記のリストに含まれる Cisco UCS C シリーズ サーバーの事前設定済みバージョンをベースとするシスコアプライアンスも、Cisco IMC UI へのアクセスを公開している場合は、この脆弱性の影響を受けます。公表時点では、次のシスコ製品が含まれていました。

- Application Policy Infrastructure Controller(APIC)サーバ
- Business Edition 6000および7000アプライアンス
- Catalyst Center Appliances (旧DNA Center)
- Cisco Telemetry Brokerアプライアンス
- Cloud Services Platform(CSP)5000シリーズ
- Common Services Platform Collector(CSPC)アプライアンス
- コネクテッドモバイルエクスペリエンス(CMX)アプライアンス
- Connected Safety and Security UCSプラットフォームシリーズサーバ
- Cyber Vision Centerアプライアンス
- Expresswayシリーズアプライアンス
- HyperFlex Edgeノード
- HyperFlexノード
- IEC6400エッジコンピューティングアプライアンス
- IOS XRv 9000アプライアンス
- Meeting Server 1000アプライアンス
- Nexusダッシュボードアプライアンス
- Prime Infrastructureアプライアンス
- Prime Network Registrar Jumpstartアプライアンス
- セキュアエンドポイントプライベートクラウドアプライアンス
- Secure Firewall Management Centerアプライアンス
- セキュアマルウェア分析アプライアンス
- Secure Network Analyticsアプライアンス
- Secure Network Serverアプライアンス
- 安全なワークロードサーバ

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。

- 5000シリーズエンタープライズネットワークコンピューティングシステム(ENCS)
- UCS CシリーズM5
- UCS EシリーズサーバM3
- UCS S シリーズ ストレージ サーバ

## 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ン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です。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。

## 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](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、本アドバイザーの URL をご用意ください。

## 修正済みリリース

次の表では、左の列にシスコソフトウェアのリリースを記載しています。右側の列は、リリースがこのアドバイザーに記載されている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最初のリリースを示しています。

### Catalyst 8300シリーズEdge uCPE

注：Cisco Catalyst 8300シリーズエッジuCPE上のCisco IMCは、Cisco Enterprise NFVインフラストラクチャソフトウェア(NFVIS)に含まれています。Cisco IMCは、NFVISのファームウェア自動アップグレードプロセスの一部としてアップグレードされます。

Cisco NFVISリリース	First Fixed Release ( 修正された最初のリリース )
4.18 以前	4.18.1

### UCS Managerソフトウェア

Cisco UCS Manager 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 )
4.1 以前	修正済みリリースに移行。
4.2	4.2(3p)
4.3	4.3 (6a)
6.0	脆弱性なし

### UCS ManagerモードのUCS BシリーズおよびXシリーズサーバ

Cisco UCSサーバ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 )
4.1 以前	修正済みリリースに移行。
4.2	4.2(3o)
4.3	4.3(5c)
6.0	脆弱性なし

#### IntersightマネージドモードのUCS Bシリーズサーバ

Cisco Intersightサーバファームウェアリリース	First Fixed Release ( 修正された最初のリリース )
4.2 より前	修正済みリリースに移行。
4.2	4.2(3l)
5.1	修正済みリリースに移行。
5.2	修正済みリリースに移行。
5.3	5.3 ( 0.250001 )
5.4	脆弱性なし
6.0	脆弱性なし

#### IntersightマネージドモードのUCS Xシリーズサーバ

Cisco Intersightサーバファームウェアリリース	First Fixed Release ( 修正された最初のリリース )
5.0	5.0(4i)
5.1	修正済みリリースに移行。
5.2	修正済みリリースに移行。
5.3	5.3 ( 0.250001 )
5.4	脆弱性なし
6.0	脆弱性なし

#### スタンドアロンモードまたはIntersightマネージドモードのUCS Cシリーズサーバ

Cisco UCSサーバ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 より前	修正済みリリースに移行。
4.2	4.2(3o)
4.3	4.3 ( 5.250001 )

Cisco UCSサーバ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 )
6.0	脆弱性なし

#### UCS ManagerモードのUCS Cシリーズサーバ

Cisco UCSサーバ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 より前	修正済みリリースに移行。
4.2	4.2(3o)
4.3	4.3(5c)
6.0	脆弱性なし

#### UCS EシリーズM6サーバ

Cisco UCSサーバ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 )
4.15 以前	4.15.2

注：事前設定バージョンのCisco UCS Cシリーズサーバに基づくCiscoアプライアンスでは、管理者はCisco IMCソフトウェアを、上の表に示した修正済みリリースのいずれかに直接アップグレードできます。手順については、『[Cisco Host Upgrade Utility User Guide](#)』を参照してください。ただし、次の表に記載されているアプライアンスは例外です。これらのアプライアンスについては、「修復」列の指示に従ってください。

シスコ ハードウェア プラットフォーム	最初の修正済みCisco IMCリリース	修復方法
Cisco Telemetry Brokerアプライアンス	4.3 ( 5.250030 )	ファームウェアアップデート <a href="#">m6-tb2300-ctb-firmware-4.3-5.250030.iso</a> を適用します。
IEC6400エッジコンピューティングアプライアンス	4.3 ( 5.250033 )	IEC6400-HUU-4.3.5.imgを使用してHUUアップグレードを適用します。
セキュアエンドポイントプライベートクラウドアプライアンス	4.3 ( 6.250053 )	バージョン4.2.5以降にアップグレードし、『 <a href="#">TechNote</a> 』に記載されている手順に従ってください。
Secure Firewall Management Centerアプライアンス	4.3 ( 6.250053 )	<a href="#">ホットフィックスI</a> を適用します。

シスコ ハードウェア プラットフォーム	最初の修正済みCisco IMCリリース	修復方法
セキュアマルウェア分析アプリケーション	4.3 ( 6.250053 )	<a href="#">アウトオブバンドファームウェアアップデートISO手順</a> を使用してファームウェアをアップデートします。
Secure Network Analyticsアプリケーション	4.3 ( 5.250030 )	アップデート <a href="#">patch-common-SNA-FIRMWARE-20250403-v2-01.swu</a> をインストールします。
Secure Network Serverアプリケーション	4.3 ( 5.250001 )	『 <a href="#">Cisco SNS 3700シリーズのファームウェアアップグレードガイド</a> 』の説明に従って、BIOSおよびHUUアップグレードを適用します。

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や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-ucs-vkvmorv-CnKrV7HK>

## 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	2025年8月27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。

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、単独の転載や意識を施した場合、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。