Cisco Integrated Management Controllerの仮想キーボードビデオモニタに保存されたクロスサイトスクリプティングの脆弱性

Medium

アドバイザリーID : cisco-sa-ucs-kvmsxss-6h7AnUyk　CVE-2025-20342
初公開日 : 2025-08-27 16:00
バージョン 1.0 : Final
CVSSスコア : 5.4
回避策 : No workarounds available
Cisco バグ ID : CSCwo77420 CSCwn43958 CSCwm57433 CSCwq34766

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、権限の低い認証されたリモートの攻撃者が、インターフェイスのユーザに対してストアド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、インターフェイスの特定のデータフィールドに悪意のあるコードを挿入することで、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、攻撃者は該当デバイスでvKVMアクセスを許可する特権を持つ有効なユーザクレデンシャルを持っている必要があります。

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-kvmsxss-6h7AnUyk

該当製品

脆弱性のある製品

公開時点では、次のシスコ製品で脆弱性のあるソフトウェアリリースが実行されている場合は、デバイスの設定に関係なく、この脆弱性の影響を受けました。

- Catalyst 8300シリーズEdge uCPE(CSCwo77420)
- Cisco UCS Managerソフトウェア(CSCwq34766)
- UCS Bシリーズブレードサーバ(CSCwm57433)
- UCS CシリーズM6、M7、およびM8ラックサーバ(CSCwn43958)
- UCS EシリーズサーバM6(CSCwo77420)
- UCS Xシリーズモジュラシステム(CSCwm57433)

上記のリストに含まれるCisco UCS Cシリーズサーバの事前に設定されたバージョンに基づくシスコアプライアンスも、Cisco IMC UIへのアクセスが可能な場合に、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

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。このアドバイザリの先頭にあるバグIDの詳細情報のセクションで、最新の情報を確認してください。

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

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。

修正済みリリース

公開時点では、次の表の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。

左側の列にはシスコソフトウェアリリース、右側の列にはリリースがこのアドバイザリ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リリースが示されています。

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)

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）
5.1	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）
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m6-tb2300-ctb-firmware-4.3-5.250030.iso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、『TechNote』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）	ホットフィックスIを適用します。
セキュアマルウェア分析アプライアンス	4.3（6.250053）	アウトオブバンドファームウェアアップデートISO手順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アプライアンス	4.3（5.250030）	アップデートpatch-common-SNA-FIRMWARE-20250403-v2-01.swuをインストールします。
Secure Network Serverアプライアンス	4.3（5.250001）	『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』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-kvmsxss-6h7AnUyk

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

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。