Cisco UCSおよびUCSベースアプライアンスのUEFIシェルセキュアブートバイパスの脆弱性

High

アドバイザリーID : cisco-sa-ucs-uefi-sb-bypass-eb6xC5GW
初公開日 : 2026-09-08 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 : CSCwt77804 CSCwu42927 CSCwu42928 CSCwt77952 CSCwt77950 CSCwt78022

CVE-2026-20293

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 UCSサーバおよびUCSベースのアプライアンスのUnified Extensible Firmware Interface(UEFI)シェル実装における脆弱性により、userまたはadminのロールを持つユーザアカウントに対して有効なクレデンシャルを持つ認証されていない攻撃者、または該当デバイスに物理的にアクセスする認証されていない攻撃者が、UEFIセキュアブートの検証チェックをバイパスし、不正なソフトウェアを実行する可能性があります。

この脆弱性は、デバイスでUEFIセキュアブートが有効な場合に、UEFIシェルでメモリ書き込みコマンドが使用できることに起因します。攻撃者は、ブート時にUEFIシェルブートオプションを選択し、利用可能なシェルコマンドを使用してUEFIメモリ変数を変更することで、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、攻撃者はプリブート環境を操作し、UEFIセキュアブート関連のメモリ値を上書きし、該当デバイスで不正なソフトウェアを実行する可能性があります。

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-ucs-uefi-sb-bypass-eb6xC5GW

該当製品

脆弱性のある製品

この脆弱性は、次のシスコ製品でUEFIセキュアブートが有効になっており、脆弱性のあるBIOSバージョンを実行している場合に影響を与えます。

- 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)(CSCwu42927)
- UCS Bシリーズブレードサーバ(CSCwt77804)
- UCS Cシリーズラックサーバ(CSCwt77804)
- UCS C845A M8ラックサーバ(CSCwt77950)
- UCS C885A M8ラックサーバ(CSCwt77952)
- UCS C880A M8ラックサーバ(CSCwt78022)
- UCS EシリーズM3サーバ(CSCwu42927)
- UCS EシリーズM6サーバ(CSCwu42928)
- UCS Sシリーズストレージサーバ(CSCwt77804)
- UCS Xシリーズモジュラシステム(CSCwt77804)
- ユニファイドエッジ(CSCwt77804)

事前設定されたバージョンのCisco UCS Cシリーズサーバをベースとするシスコのアプライアンスでも、UEFIセキュアブートがサポートされており、キーボード、ビデオ、マウス(KVM)または仮想KVMコンソールへのアクセスが可能な場合は、この脆弱性の影響を受けます。本ドキュメントの発行時点で、これに該当するシスコ製品は次のとおりです。

- Application Policy Infrastructure Controller（APIC）サーバー
- Cisco Telemetry Broker アプライアンス
- HyperFlex エッジノード
- HyperFlex ノード
- IEC6400 エッジ コンピューティング アプライアンス
- Cisco IOS XRv 9000 M7 アプライアンス
- Nexus Dashboard アプライアンス
- セキュアEメールゲートウェイ[1]
- Secure Email and Web Manager(SEM)[1]
- Cisco Secure Endpoint Private Cloud アプライアンス
- Secure Firewall Management Center（FMC）アプライアンス
- Cisco Secure Malware Analytics アプライアンス
- Cisco Secure Network Analytics アプライアンス
- Secure Network Server（ISE SNS）アプライアンス
- セキュアWebアプライアンス[1]

1. これらのアプライアンスの脆弱性を悪用するには、物理的なKVMアクセスが必要です。これにより、これらのプラットフォームでの攻撃ベクトルが大幅に減少します。

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。

詳細

UEFIシェルは、デバッグ、スクリプト、およびさまざまなブートオプションを制御するためのコマンドを提供するコマンドラインインターフェイスです。UEFIブートモードのCisco UCSサーバのブートオプションとして使用できます。

UEFIシェルには、メモリの変更を可能にする複数のコマンドが含まれています。デバイス上でUEFIセキュアブートが有効になっている場合、このようなコマンドが使用できることで、攻撃者はUEFIセキュアブート関連のメモリ値の上書きを含むプリブート環境を操作し、UEFIセキュアブート検証をバイパスできる可能性があります。

この脆弱性を解決するため、デバイスでUEFIセキュアブートが有効になっている場合、メモリの変更を可能にするUEFIシェルコマンドはシェルから削除されます。

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。この脆弱性を修正して、このアドバイザリで説明されている障害の発生を防ぐために、お客様はこのアドバイザリで説明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お勧めします。

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最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

5000 シリーズ ENCS

注：Cisco 5000シリーズENCSでCisco Integrated Management Controller(IMC)およびBIOSをアップグレードするには、プラットフォームでCisco Enterprise NFVインフラストラクチャソフトウェア(NFVIS)をアップグレードする必要があります。Cisco IMCおよびBIOSは、ファームウェ

アの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）
4.15 以前	4.15.7（2026年10月）

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

Cisco UCS サーバー 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）
4.3 より前	修正済みリリースに移行。
4.3	4.3(6h)[1]
6.0	6.0(2d)[1]

1. これらのリリースには、Cisco UCS BシリーズM5サーバに対する修正は含まれていません。これらのプラットフォームの修正は、2026年9月にリリースされる予定です。

Intersight 管理対象モードの UCS B シリーズ サーバー

Cisco Intersight サーバー 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）
5.4 より前	修正済みリリースに移行。
5.4	5.4(0.260050)[1]
6.0	6.0（2.260143）

1. このリリースには、Cisco UCS BシリーズM5サーバに対する修正は含まれていません。これらのプラットフォームに対する修正は、次回のリリース（2026年9月）で提供される予定です。

Intersight 管理対象モードの UCS X シリーズ サーバー

Cisco Intersight サーバー 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）
5.4 より前	修正済みリリースに移行。
5.4	5.4（0.260042）
6.0	6.0（2.260143）

UCS C845A M8ラックサーバ

Cisco UCS サーバー 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）
2.0	リリース番号未定（2026年10月）

UCS C880A M8ラックサーバ

Cisco UCS サーバー 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）
4.0	4.0（2.260004）

UCS C885A M8ラックサーバ

Cisco UCS サーバー 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）
1.2 以前	リリース番号未定（2026年9月）

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M5ラックサーバ

Cisco UCS サーバー 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(3r)
4.3	4.3（2.260020）

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M6、M7、M8ラックサーバ

Cisco UCS サーバー 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(3r)
4.3	4.3（6.260054）
6.0	6.0(2.260143)[1]

1. 修正済みの 6.0(2.260143) Host Upgrade Utility（HUU）ISO リリースには、Cisco IMC 6.0(2.260094) のパッケージリリースが含まれています。 この修正済みリリースにアップグレードすると、Cisco IMC UIの ダッシュボードページに、 ファームウェアバージョンとして 6.0(2.260094)が表示されます。 [管理（Administration）] > [ファームウェア管理（Firmware Management）] の下の [最後に使用されたHSUバンドル（Last HSU bundle used）] フィールドに、修正済みの 6.0(2.260143) リリースが表示されます。

UCS Manager モードの UCS C シリーズ サーバー

Cisco UCS サーバー 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(3s)
4.3	4.3(6h)[1]
6.0	6.0(2d)[1]

1. これらのリリースには、Cisco UCS CシリーズM5サーバに対する修正は含まれていません。これらのプラットフォームの修正は、2026年9月にリリースされる予定です。

UCS EシリーズM3サーバ

Cisco UCSE BIOSリリース	First Fixed Release（修正された最初のリリース）
4.0 以前	4.04[1]（2026年9月）

1. 修正済みの4.04 BIOSリリースは、『Cisco UCS E-Series Integrated Management Controller GUIコンフィギュレーションガイド』の「ファームウェアの管理」セクションに記載されている手順を使用して、任意のCisco IMC 3.2リリースを実行しているUCS EシリーズM3サーバにインストールできます。

UCS EシリーズM6サーバ

Cisco UCSE 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	4.15.4-b[1]（2026年9月）

1. 修正済みの4.15.4-b Host Upgrade Utility(HUU)ISOリリースには、修正済みの2.06 BIOSリリースが含まれています。

UCS S シリーズ ストレージ サーバー

Cisco UCS サーバー 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）
4.3 より前	修正済みリリースに移行。
4.3	4.3（6.260054）

Unified Edge

Cisco UCS XEシリーズ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）
6.0	6.0（2.260143）

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アプライアンスの場合、管理者は上記の表に記載された修正済みリリースのいずれかを使用して、Cisco IMCおよびBIOSソ

フトウェアの直接アップグレードを実行できます。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、「修復方法」の欄にある手順に従ってください。

シスコ ハードウェア プラットフォーム	最初の修正済みファームウェアリリース	修復方法
Cisco Telemetry Broker アプライアンス	6.0(2.260143)[1]	ファームウェアの更新 CTB-FIRMWARE-6.0.2.260143-M6.iso をインストールします。
IEC6400 エッジ コンピューティング アプライアンス	4.3（6.260054）	IEC6400-HUU-4.3.6-260054.imgを使用してHUUアップグレードを適用します。
Cisco IOS XRv 9000 M7 アプライアンス	6.0(2.260143)[1]	Cisco IOS XRソフトウェアリリース26.3.1にアップグレードしてから、Cisco IOS XR CLIからアプライアンスファームウェアをアップグレードしてください。
セキュアなEメールゲートウェイ	4.3（2.260020）	ファームウェアアップデートパッケージのインストール（2026年10月）
Cisco Secure Email and Web Manager	4.3（2.260020）	ファームウェアアップデートパッケージのインストール（2026年10月）
Cisco Secure Endpoint Private Cloud アプライアンス	4.3(2.260020) (M5) 4.3(6.260054) (M6)	TechNote に記載されている手順に従います。
Secure Firewall Management Center（FMC）アプライアンス	4.3(2.260020) (M5) 6.0(2.260143)[1] (M6、M8)	ホットフィックス GA を適用します。
Cisco Secure Malware Analytics アプライアンス	4.3(2.260020) (M5) 4.3(6.260054) (M6)	アウトオブバンド ファームウェアの更新 ISO の手順を使用して、ファームウェアを更新します。
Cisco Secure Network Analytics アプライアンス	4.3(2.260020) (M5) 6.0(2.260143)[1] (M6)	M5 の場合、ファームウェアの更新 patch-common-SNA-FIRMWARE-4.3.2.260020-M5-v2-01.swu をインストールします。 M6 の場合、ファームウェアの更新 patch-common-SNA-FIRMWARE-6.0.2260143-M6-v2-01.swu をインストールします。

シスコ ハードウェア プラットフォーム	最初の修正済みファームウェアリリース	修復方法
Secure Network Server（ISE SNS）アプライアンス	4.3(2.260020) (M5) 6.0(2.260143)[1] (M6、M8)	Cisco Secure Network Server 3600 シリーズ、Cisco Secure Network Server 3700 シリーズ、または Cisco Secure Network Server 3800 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 のアップグレードを適用します。
セキュアWebアプライアンス	4.2(3r)(M5) 4.3(6.260054) (M6)	ファームウェアアップデートパッケージのインストール（2026年10月）

1. 修正済みの 6.0(2.260143) ファームウェアリリースには、Cisco IMC 6.0(2.260094) のパッケージリリースが含まれています。この修正済みリリースにアップグレードすると、Cisco IMC UIのダッシュボードページに、 ファームウェアバージョンとして6.0(2.260094)が表示されます。Administration > Firmware Managementの下の Last HSU bundle usedフィールドに、使用されている特定のアプライアンスと修復によっては、修正済みの6.0(2.260143)リリースまたは N/Aが表示される場合があります。

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 は、このアドバイザリで説明されている脆弱性に対してコンセプト実証エクスプロイトコードが利用可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

シスコは、この脆弱性を報告していただいたEclypsium社のStas Lyakhov氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-uefi-sb-bypass-eb6xC5GW

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9月8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。