

Cisco Integrated Management Controller のバッファ オーバーフローにおける脆弱性



アドバイザリーID : [cisco-sa-20190821-imc-CVE-2019-bo-1871](#)

初公開日 : 2019-08-21 16:00

バージョン 1.0 : Final

CVSSスコア : [7.2](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvo36122](#)

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 Cisco IMC 設定ユーティリティのインポートにおける脆弱性により、認証されたりモートの攻撃者が、該当デバイスでルート権限を使用して、サービス妨害 (DoS) 状態を発生させ、任意のコマンドを実装する可能性があります。

この脆弱性は、import-config プロセスによる範囲チェックが不適切なことに起因します。攻撃者は、悪意のあるパケットを該当デバイスに送信することによって、本脆弱性を不正利用する可能性があります。パケットを処理する際に、バッファ オーバーフローが攻撃に利用できる状態で発生する場合があります。エクスプロイトに成功すると、攻撃者は昇格された特権を使用して、該当デバイスに任意のコードを実装することができます。

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-20190821-imc-bo>

該当製品

脆弱性のある製品

この脆弱性は、Cisco IMC ソフトウェアの脆弱性のある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。

- スタンドアロン モードになっている UCS C シリーズおよび S シリーズ サーバ

- UCS E シリーズ サーバ
- 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) プラットフォーム

該当するソフトウェア 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](#)」の項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、この脆弱性が UCS Manager によって管理される以下の Cisco FI 接続サーバには影響を与えないことを確認しました。

- Cisco UCS-B シリーズ サーバ
- Cisco UCS C シリーズ サーバ
- Cisco UCS S シリーズ 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。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。

[ソフトウェアのアップグレードを検討する](#)際には、[シスコのセキュリティアドバイザリおよびアラート (Cisco Security Advisories and Alerts)] 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 Cisco Service Contract 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 POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

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

Cisco UCS C シリーズおよび S シリーズ サーバ

次の表に示すように、適切な UCS C シリーズおよび S シリーズ 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。

Cisco IMC 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)
1.4	脆弱性なし
1.5	脆弱性なし
2.0	脆弱性なし
3.0	3.0(4k)
4.0	4.0(2f)、4.0(4b)

Cisco IMC ソフトウェアは、Cisco.com の [Software Center にアクセスし、次の手順でダウンロードできます。](#)

1. [すべてを参照 (Browse All)] をクリックします。
2. [サーバ: ユニファイドコンピューティング (Servers - Unified Computing)] > [UCS Cシリーズラックマウントスタンドアロンサーバソフトウェア (UCS C-Series Rack-Mount Standalone Server Software)] にアクセスします。
3. 右側のペインで、適切な Cisco UCS C シリーズ プラットフォームを選択します。
4. [ソフトウェアの種類を選択 (Select a Software Type)] ページで、[ユニファイドコンピューティングシステム(UCS)サーバファームウェア (Unified Computing System (UCS) Server Firmware)] をクリックします。
5. ページの左側のペインを使用してリリースにアクセスします。

Cisco UCS E シリーズ サーバ

シスコは、Cisco UCS E シリーズ サーバ向けの Cisco IMC ソフトウェア リリース 3.2(8) でこの脆弱性を修正しました。

このソフトウェアは Cisco.com の [Software Center にアクセスし、次の手順でダウンロードできます。](#)

1. [すべてを参照 (Browse All)] をクリックします。
2. [サーバ: ユニファイドコンピューティング (Servers - Unified Computing)] > [UCS E シリーズソフトウェア (UCS E-Series Software)] にアクセスします。
3. 右側のペインで、適切な Cisco UCS E シリーズ プラットフォームを選択します。
4. [ソフトウェアの種類を選択 (Select a Software Type)] ページで、[ユニファイドコンピューティングシステム(UCS)サーバファームウェア (Unified Computing System (UCS) Server Firmware)] をクリックします。
5. ページの左側のペインを使用してリリースにアクセスします。

Cisco 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) プラットフォーム

シスコは、Cisco 5000 シリーズ ENCS プラットフォーム向けの Cisco IMC ソフトウェア リリース 3.2(8) でこの脆弱性を修正しました。

このソフトウェアは Cisco.com の [Software Center にアクセスし、次の手順でダウンロードできます。](#)

1. [すべてを参照 (Browse All)] をクリックします。
2. [ルータ (Routers)] > [ネットワーク機能の仮想化 (Network Functions Virtualization)] > [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 (5000 Series Enterprise Network Compute System)] にアクセスします。
3. 右側のペインで、適切な ENCS プラットフォームを選択します。
4. [ソフトウェアの種類を選択 (Select a Software Type)] ページで、[ENCSソフトウェア (ENCS Software)] をクリックします。
5. ページの左側のペインを使用してリリースにアクセスします。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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を確認していません。

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-20190821-imc-bo>

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	2019 年 8 月 21 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。