Cisco Integrated Management Controllerの認証バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-cimc-auth-zWkppJxL
初公開日 : 2020-11-04 16:00
最終更新日 : 2021-02-26 15:37
バージョン 1.1 : Final
CVSSスコア : 5.4
回避策 : No workarounds available
Cisco バグ ID : CSCvv07287 CSCvv95114

CVE-2020-26063

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APIエンドポイントの脆弱性により、認証されたリモートの攻撃者が権限をバイパスし、権限のない脆弱なシステムでアクションを実行する可能性があります。

この脆弱性は、APIエンドポイントでの不適切な認証チェックに起因します。攻撃者は、悪意のある要求をAPIエンドポイントに送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は該当システムからファイルをダウンロードしたり、該当システムの限定された設定オプションを変更したりする可能性があります。

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-cimc-auth-zWkppJxL

該当製品

脆弱性のある製品

公開時点では、この脆弱性はCisco Integrated Management Controllerリリース4.0(4h)C以前を実行する次のシスコ製品に影響を与えました。

- 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）プラットフォーム

- スタンドアロンモードになっている UCS C シリーズ ラックサーバ
- UCS E シリーズ サーバ

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。

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アップグレード ソリューション一式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

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。

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

シスコは、この脆弱性を報告していただいたF-Secure ConsultingのLeonidas Tsausis氏とThomas Large氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-zWkppJxL

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	追加のシスコ製品への影響に関する情報を追加。	脆弱性が存在する製品	Final	2021年2月26日
1.0	初回公開リリース	—	Final	2020 年 11 月 4 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。