Cisco Integrated Management Controller Supervisor、Cisco UCS Director、および Cisco UCS Director Express for Big Data の SCP ユーザのデフォルト クレデンシャルにおける脆弱性

Critical

アドバイザリーID : cisco-sa-20190821-imcs-usercred

初公開日 : 2019-08-21 16:00

最終更新日 : 2019-08-30 12:38

バージョン 1.1 : Final

CVSSスコア : 9.8

回避策 : Yes

Cisco バグ ID : CSCvp19251

CVE-2019-1935

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) Supervisor、Cisco UCS Director、および Cisco UCS Director Express for Big Data の脆弱性により、認証されていないリモートの攻撃者が、デフォルトのユーザ クレデンシャルがある SCP ユーザ アカウント（*scpuser*）を使用して該当システムの CLI にログインする可能性があります。

この脆弱性は、文書化されたデフォルトのアカウントが存在し、そのアカウントに対する文書化されていないデフォルトのパスワードと不正な権限設定があることに起因します。 このアカウントのデフォルトのパスワードの変更は、製品のインストール時には適用されません。 攻撃者は、そのアカウントを使用して該当システムにログインすることで、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 *scpuser* アカウントの権限で任意のコマンドを実行することができます。 これには、システムのデータベースへの完全な読み取り/書き込みアクセス権が含まれます。

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ました。 本脆弱性に対処する回避策がいくつかあります。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-usercred

該当製品

脆弱性のある製品

本脆弱性は、以下のシスコ製品に影響します。

Cisco IMC Supervisor のリリース：

- 2.1
- 2.2.0.0 ~ 2.2.0.6

Cisco UCS Director のリリース：

- 6.0
- 6.5
- 6.6.0.0 および 6.6.1.0
- 6.7.0.0 および 6.7.1.0

Cisco UCS Director Express for Big Data のリリース：

- 3.0
- 3.5
- 3.6
- 3.7.0.0 および 3.7.1.0

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

回避策

scpuser アカウントのカスタム パスワードを [管理（Administration）] > [ユーザとグループ（Users and Groups）] > [SCPユーザ設定（SCP User Configuration）] で設定すると、この脆弱性のエクスプロイトを防止できます。

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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ます。 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、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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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 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、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性は、次のソフトウェア リリースで修正されています。

- Cisco Integrated Management Controller Supervisor 2.2.1.0 以降のリリース
- Cisco UCS Director 6.7.2.0 以降のリリース（推奨リリース： 6.7.3.0）
- Cisco UCS Director Express for Big Data 3.7.2.0 以降のリリース（推奨リリース： 3.7.3.0）

Cisco IMC Supervisor 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）] > [Integrated Management Controller (IMC) Supervisor（Integrated Management Controller (IMC) Supervisor）] > [IMC Supervisor 2.x] の順に選択します。
3. [IMC Supervisor 2.x] 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 Director 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 Director] > [UCS Director 6.7] の順に選択します。
3. [UCS Director 6.7] 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 Director Express for Big Data 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 Director] > [UCS Director Express for Big Data 3.7] の順に選択します。
3. [UCS Director Express for Big Data 3.7] 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

ペドロ Ribeiro セキュリティ研究者は GitHub 彼のリポジトリのこの脆弱性の詳細を送達し、また対応する Metasploit モジュールをリリースしました。

出典

iDefense の Vulnerability Contributor Program にこの脆弱性を報告していただいた個人のセキュリティ研究者である Pedro Ribeiro 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-usercred

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	公共エクスプロイト コードの公示およびアベイラビリティを更新しました。	不正利用事例と公式発表	最終版	2019-August-30
1.0	初回公開リリース		最終版	2019 月 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。