

Cisco Elastic Services Controller サービス ポータルにおける不正アクセスの脆弱性

High

アドバイザリーID : cisco-sa-20180221-esc1

[CVE-2018-0130](#)

初公開日 : 2018-02-21 16:00

最終更新日 : 2019-02-08 14:15

バージョン 1.1 : Final

CVSSスコア : [7.3](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvg30884](#)

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 Elastic Services Controller ソフトウェアの Web ベース サービス ポータルによる JSON Web トークン使用の脆弱性により、該当システムに対する管理アクセス権を、未認証のリモート攻撃者に取得される可能性があります。

この脆弱性は、該当ソフトウェアの Web ベース サービス ポータルにスタティックなデフォルトのクレデンシャルが存在していることに起因します。この脆弱性は、攻撃者が該当ソフトウェアのイメージからクレデンシャルを抽出し、そのクレデンシャルを使用して、該当ソフトウェアのその他のインストールの Web ベース サービス ポータル用に有効な管理セッショントークンを生成することで、不正利用される可能性があります。不正利用が成功すると、該当システムの Web ベース サービス ポータルに対する管理アクセス権を攻撃者に取得され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ました。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180221-esc1>

該当製品

脆弱性のある製品

この脆弱性は、Cisco Elastic Services Controller ソフトウェア リリース 3.0.0 に影響します。

システムで実行されている Cisco Elastic Services Controller (ESC) ソフトウェア リリースを確認するには、ESC CLI で管理者権限で `esc_version` コマンドを実行し、`version` フィールドの出力を参照します。システムで Cisco ESC ソフトウェア リリース 4.0.0 が実行されている場合のコマンド出力は、次の例のようになります。

```
[admin@esc-4-0-0-80-uut ~]$ esc_version
    version : 4.0.0
    release : 80
yang.model.version : 152
    repo : ssh://esc-repo
    branch : master
```

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

シスコは、この脆弱性がリリース 3.0.0 より前の Cisco Elastic Services Controller ソフトウェア リリースには影響を与えないことを確認しました。

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、[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、Cisco Elastic Services Controller ソフトウェア リリース 3.1.0 以降で修正されています。お客様の側で最新のソフトウェア リリースにアップグレードする必要があります。アップグレードするには、Cisco.com の [Software Center](#) にアクセスして、[製品 (Products)] > [クラウドおよびシステム管理 (Cloud and Systems Management)] > [サービス管理およびオーケストレーション (Service Management and Orchestration)] > [Elastic Services Controller] の順に移動します。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) では、本アドバイザリに記載されている脆弱性のエクスプロイト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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180221-esc1>

改訂履歴

バージョン	説明	セクション	ステータ	Date
-------	----	-------	------	------

ン			ス	
1.1	Software Center への更新済リンク	修正済みリリース	最終版	2019-February-08
1.0	初回公開リリース		最終版	2018年2月21日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。