Cisco Elastic Services Controller Unauthorized Access Vulnerability

Critical

アドバイザリーID : cisco-sa-20170705-esc2

初公開日 : 2017-07-05 16:00

バージョン 1.0 : Final

CVSSスコア : 9.8

回避策 : Yes

Cisco バグ ID : CSCvc76627

CVE-2017-6713

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 (ESC) の Play Framework の脆弱性により、認証されていないリモート攻撃者が該当システムへのフル アクセス権を取得する可能性があります。

この脆弱性は、Cisco ESC UI の静的なデフォルト クレデンシャルがインストール環境間で共有されることに起因します。 Cisco ESC の既存のインストール環境から静的なクレデンシャルを取得できる攻撃者は、ESC Web UI のすべてのインスタンスへのアクセスを可能にする管理セッション トークンを生成する可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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。
705-esc2

該当製品

修正済みソフトウェア

この脆弱性は、Cisco Elastic Services Controller の 2.3.1.434 より前および 2.3.2 より前のリリースに影響します。

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。

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017-July-05

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。