Cisco Registered Envelope Service クロスサイト スクリプティング脆弱性

Medium	**アドバイザリーID :** cisco-sa-20180307-res **初公開日 :** 2018-03-07 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 5.4 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvg74126	CVE-2018-0208

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 Registered Envelope Service のウェブベースの管理インターフェイスの脆弱性は影響を受けたサービスのウェブベースの管理インターフェイスのユーザに対してクロスサイト スクリプティング（XSS）不正侵入を行なう認証される、リモート攻撃者可能にする可能性があります。

脆弱性は影響を受けたサービスのウェブベースの管理インターフェイスによって処理されるユーザが指定する入力の不十分な検証が原因です。 攻撃者はインターフェイスのユーザの悪意のあるリンクをクリックするように説得によってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が任意スクリプト コードをインターフェイスという点において実行するか、または敏感なブラウザ・ベースの情報にアクセスすることを可能に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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-res

該当製品

脆弱性のある製品

この脆弱性は基づくクラウドである Cisco Registered Envelope Service に影響を与えます。

該当するソフトウェア リリースについての情報に関しては、この状況報告の上で Cisco バグ ID を参照して下さい。

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。

詳細

Cisco Registered Envelope Service は非常に高度、クラウド ベース、キー サービスです。 準拠性必要条件を満たすか、通信を保護するか、または追加インフラストラクチャに投資しないで知的 財産、この適用範囲が広いおよび拡張が容易なサービス サービス支援をメッセージング必要条件保護する必要があるかどうか。

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

パブリケーションの時に、修正済みソフトウェアはこの脆弱性に Cisco Registered Envelope Service に提供されました。 修正済みソフトウェアリリースについての最新情報およびほとんどの詳細な情報に関しては、この状況報告の上で Cisco バグ ID を参照して下さい。

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

Cisco はこの脆弱性を報告するために Hindustan 大学からのセキュリティ研究者に感謝することを Rahul Raj 望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-res

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-March-07

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。