Cisco Unity Connection によって反映されるクロスサイト スクリプティング脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170906-cuc **初公開日 :** 2017-09-06 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.1 **回避策 :** Yes **Cisco バグ ID :** CSCvf25345	CVE-2017-12212

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 Unity Connection の Web フレームワークの脆弱性はリモート攻撃者非認証が影響を受けたシステムの Webインターフェイスのユーザに対して反映されたクロスサイト スクリプティング（XSS）攻撃を行なうようにする可能性があります。

脆弱性は HTTP GET および HTTP POST メソッドによって影響を受けたソフトウェアに通じるある特定のパラメータの不十分な入力の検証が原因です。 ユーザを攻撃者供給されたリンクに従うように確信できる攻撃者は影響を受けたサイトという点においてユーザーのブラウザーの任意スクリプトか HTML コードを実行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-20170906-cuc

該当製品

修正済みソフトウェア

この脆弱性は Cisco Unity Connection に影響します。 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、このアドバイザリの上で 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。

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017-September-06

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。