

Cisco Identity Services Engine 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-20190904-ise-xss	CVE-2019-12644
m	初公開日 : 2019-09-04 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 6.1	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvp98851	

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 Identity Services Engine (ISE) ソフトウェアのウェブベースの管理インターフェイスの脆弱性はリモート攻撃者非認証が影響を受けたデバイ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) 攻撃を行なうようにする可能性があります。

影響を受けたデバイスのウェブベースの管理インターフェイスがきちんとユーザが指定する入力を検証しないので存在する脆弱性。攻撃者はユーザの巧妙に細工された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に影響を受けた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。

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-20190904-ise-xss>

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性は Cisco ISE ソフトウェア リリースにリリース 2.6.0 より先に該当しました。

最も完全な、現在の情報についてはこのアドバイザリの上でバグIDの詳細 セクションを参照して下さい。

脆弱性を含んでいないことが確認された製品

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である。

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

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。

修正済みリリース

出版物の時に、Cisco ISE ソフトウェアリリース 2.6.0 およびそれ以降はこの脆弱性のための修正が含まれていました。

最も完全な、現在の情報についてはこのアドバイザリの上でバグIDの詳細 セクションを参照して下さい。

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 STM ソリューションの Krzysztof Przybylski に感謝することを望みます。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-ise-xss>

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019-September-04

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。