

Cisco Identity Services Engine ゲスト門脈クロス 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-20170705-ise2	CVE-2017-6734
m	初公開日 : 2017-07-05 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 5.4	
	回避策 : Yes	
	Cisco バグ ID : CSCvd74794	

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影響を受けたデバイスの Web 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ソフトウェアのウェブベースの管理インターフェイスによって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、または攻撃者が敏感なブラウザ ベースの情報にアクセスするようにことを可能にする可能性があります。

クロスサイト スクリプティング攻撃およびこれらの脆弱性を不正利用するのに使用されるメソッドについてのその他の情報に関しては Cisco によって加えられる軽減情報 [知識クロスサイト スクリプティング 脅威ベクター](#) および OWASP 参照ページ [クロスサイト スクリプティング \(XSS\) を調べて下さい](#)。

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。
[705-ise2](#)

影響を受ける製品

脆弱性が存在する製品

この脆弱性は Cisco Identity Services Engine (ISE) ソフトウェアに影響を与えます。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、このアドバイザリの上で Cisco バグ ID を参照して下さい。

脆弱性が存在しない製品

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。

細部

回避策

この脆弱性に対処する回避策はありません。

固定ソフトウェア

修正済み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。

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、現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。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。

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。

ソース

Cisco はこの脆弱性を発見することおよび報告するために Rits 情報 セキュリティのセキュリティ研究者に感謝することをリチャード ドルトン望みます。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-ise2>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース		最終版	2017-July-05

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。