

Cisco Umbrella 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-20190417-umbrella-xss	CVE-2019-1792
	初公開日 : 2019-04-17 16:00	
	最終更新日 : 2019-05-08 15:46	
	バージョン 1.1 : Final	
	CVSSスコア : 6.1	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvo32441	

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 Umbrella の Block ページ URL の脆弱性はリモート攻撃者非認証が Umbrella によって保護されたネットワーク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。

脆弱性はそのページに通じる入力パラメータ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をもって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-20190417-umbrella-xss>

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 Umbrella 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、このアドバイザリーの上で 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

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にである。

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

Cisco Umbrella は予防的に この アドバイザリに記載される 脆弱性を当てる必要な操作を実行された。Cisco はこれらの更新および変更が Cisco 管理されたインフラストラクチャに加えられるのでこの脆弱性を解決するために必要なソフトウェア アップデートがやコンフィギュレーション変更が顧客操作を必要としないことを判別しました。顧客は現在の治療ステータスかソフトウェア バージョンを判別するためにクラウド サービスの GUI のヘルプ セクションを参照することができます。

顧客は質問に必要なならば答えるのを助けるように Cisco Technical Assistance Center (TAC) が契約整備プロバイダに連絡するように勧告されます。

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独立した セキュリティ研究者に感謝することをザカリー Swanson 望みます。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-umbrella-xss>

改訂履歴

バージョン	説明	セクション	ステータ	Date
-------	----	-------	------	------

ン			ス	
1.1	Cisco Umbrella が基づくクラウドであることを示される。注目されるこの脆弱性に対処するように操作が顧客によって要求されない。	「該当製品」、「修正済みソフトウェア」	最終版	2019-May-08
1.0	初回公開リリース		最終版	2019年4月17日

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。