Cisco UCS Central ソフトウェアの多重 脆弱点

Medium	**アドバイザリーID :** cisco-sa-20171129-ucs-central **初公開日 :** 2017-11-29 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 :** CSCvf71986 CSCvf71978	CVE-2017-12348 CVE-2017-12349

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 UCS Central 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多重 脆弱点はリモート攻撃者がクロスサイト スクリプティング（XSS）攻撃を影響を受けたインターフェイスのユーザに対して行なうまたは影響を受けたインターフェイスのユーザからの有効なセッションID を乗っ取ることを可能にする可能性があります。

これらの脆弱性に関する詳細については、この Security Advisory の" Details " セクションを参照して下さい。

これら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-20171129-ucs-central

該当製品

脆弱性のある製品

これらの脆弱性は最初の修正済みリリース前に Cisco UCS Central ソフトウェアのすべてのリリースに該当します。 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。

詳細

Cisco UCS Central 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 2 脆弱性はリモート攻撃者がクロスサイト スクリプティング（XSS）攻撃を影響を受けたインターフェイスのユーザに対して行なうまたは影響を受けたインターフェイスのユーザからの有効なセッションID を乗っ取ることを可能にする可能性があります。

脆弱性は互いに依存していません; 脆弱性の 1 の不正利用が他の脆弱性を不正利用するために必要となりません。 さらに、脆弱性の 1 から影響を受けするソフトウェア リリースは他の脆弱性から影響を受けしないかもしれません。

脆弱性についての詳細は次の通りです。

Cisco UCS Central ソフトウェア クロスサイト スクリプティング脆弱性

Cisco UCS Central 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ユーザに対して 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。 攻撃者は影響を受けた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、または攻撃者がユーザのシステムの敏感なブラウザ 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。

この脆弱性を不正利用するために、攻撃者は影響を受けたソフトウェアに有効 な ユーザ 資格情報のためのおよび認証するがなければなりません。

従ってこの脆弱性が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の耐久性があるスクリプトを実行するのに不正利用し、ターゲットとされたユーザ以外ユーザに影響を与えるのに活用 することができません。

この脆弱性のための CVE ID は次のとおりです: CVE-2017-12348

この脆弱性のためのセキュリティ へ の 影響 定格（ ）は次のとおりです: 中間

Cisco UCS Central ソフトウェア セッション固定脆弱性

Cisco UCS Central 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セッション管理 機能の脆弱性はリモート攻撃者非認証が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のユーザからの有効なセッションID を乗っ取るようにする可能性があります。

ユーザがソフトウェアに認証を受ける時影響を受けたソフトウェアがユーザセッションに新しいセッションID を割り当てないので存在 する脆弱性。 攻撃者は乗っ取られたセッションID の使用によってソフトウェアのウェブベースの管理インターフェイスを通って影響を受けたソフトウェアに接続するのに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認証済みユーザのブラウザー セッションを乗っ取ることを可能にする可能性があります。

この脆弱性のための CVE ID は次のとおりです: CVE-2017-12349

この脆弱性のための次のとおりです: 中間

回避策

これら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

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、および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不正利用事例とその公表は確認しておりません。

出典

Cisco はこれらの脆弱性を報告するためにアプリケーションセキュリティ コンサルタント Indrajith.A.N に感謝することを望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-ucs-central

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017-November-29

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。