

Cisco WebEx Meetings および Cisco Webex ミーティング サーバ HTML インジェクト脆弱性

Medium アドバイザリーID : cisco-sa-webex-html-BJ4Y9tX [CVE-2020-3345](#)
初公開日 : 2020-07-15 16:00
最終更新日 : 2020-07-20 14:31
バージョン 1.1 : Final
CVSSスコア : [4.3](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCvt75616](#)
[CSCvt75607](#) [CSCvu00484](#)
[CSCvu06679](#)

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 WebEx Meetings および Cisco Webex ミーティング サーバのある特定の Web ページの脆弱性はリモート攻撃者非認証がブラウザという点において Web ページを修正するようになる可能性があります。

脆弱性は影響を受けたページ内のパラメーター値の不適切なチェックが原因です。攻撃者は影響を受けたパラメータに HTML コードを渡すように設計されているユーザの巧妙に細工されたリンクに従う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可能性としては悪意のある Web サイトにユーザをリダイレクトするために Web ページの内容を変えることを可能にする可能性がありますまたは攻撃者はそれ以上のクライアント側の不正侵入を行なうためにこの脆弱性にてこ入れ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-webex-html-BJ4Y9tX>

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性はリリース 40.6.0 および Cisco Webex ミーティング サーバがよりリリース 4.0 MR3 先にリリースするより Cisco WebEx Meetings リリースに先に該当しました。

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[脆弱性のある製品](#)セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

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、[シスコ セキュリティ アドバイザリ 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

パブリケーション、Cisco WebEx Meetings リリース 40.6.0 および以降および Cisco Webex ミーティング サーバ リリースの時に 4.0 MR3 はおよび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 Certego IRT のガブリエレ Pippi に感謝することを望みます。Ciscoは独自にこの脆弱性を報告するためにセキュリティ研究者に感謝することを Prasenjit Kanti ポール望みます。Ciscoはまた独自にこの脆弱性を報告するために Shahriar Yazdipour に感謝することを望みます。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-html-BJ4Y9tX>

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	またこの脆弱性に対処する追加された Cisco バグ ID CSCvu06679。	Header	最終版	2020-JUL-20
1.0	初回公開リリース		最終版	2020-JUL-15

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。