Cisco Meeting Server コマンド インジェクトおよび特権 拡大脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170823-cms **初公開日 :** 2017-08-23 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.7 **回避策 :** Yes **Cisco バグ ID :** CSCvf53830	CVE-2017-6794

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 Meeting Server の CLI コマンド解析コードの脆弱性はコマンド インジェクトを行い、 *定着* する特権を増やす認証された、ローカル攻撃者を可能にする可能性があります。 攻撃者は有効な管理者の資格情報とのアプリケーションに最初に認証する必要があります。

脆弱性はある特定のコマンドのための CLI で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アプリケーションに認証し、Cisco Meeting Server CLI で実行のために巧妙に細工された CLI コマンドを入れることによってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者がコマンド インジェクトを行い、 *定着するために*特権レベルを増やす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。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170823-cms

該当製品

修正済みソフトウェア

Cisco Meeting Server ソフトウェア バージョンで前に存在 し、2.0、2.1、および 2.2 を含まれているこの脆弱性。

管理者はデバイスが影響を受けていたかどうか確認するために Cisco Meeting Server の CLI か

らのシステム構成をチェックできます。 管理者は **version コマンドの**使用によってソフトウェア バージョンを判別できます。 この例では、コマンド 出力はソフトウェア バージョン 2.0.6 を実行するデバイスのバージョンを以下に示します:

```
system> version
2_0_6
```

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。

改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	初回公開リリース		Final	2017-August-23

利用規約