Cisco Meeting Server TURN Server Unauthorized Access and Information Disclosure Vulnerability

Critical

アドバイザリーID : cisco-sa-20170913-cmsturn

初公開日 : 2017-09-13 16:00

バージョン 1.0 : Final

CVSSスコア : 9.1

回避策 : Yes

Cisco バグ ID : CSCvf51127

CVE-2017-12249

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（CMS）に組み込まれた Traversal Using Relay NAT（TURN）サーバの脆弱性により、認証されたリモート攻撃者が該当システム内のコンポーネントまたは機密情報に対して認証なしでのアクセスまたは不正アクセスを行う可能性があります。

この脆弱性は TURN サーバの不適切なデフォルト設定に起因し、該当システムの内部インターフェイスおよび外部インターフェイスのポートが公開される可能性があります。 使用する導入モデルと CMS サービスによっては、攻撃者は TURN サーバを使用して該当デバイスの Call Bridge、Web ブリッジ、またはデータベース クラスタに不正な接続を実行することにより、この脆弱性を不正利用する可能性があります。 不正利用に成功すると、攻撃者は該当システムの Call Bridge またはデータベース クラスタに認証なしのアクセスを行うか、または該当システムの機密情報への不正アクセスを行う可能性があります。 この脆弱性を不正利用するには、攻撃者は該当システムの TURN サーバの有効なクレデンシャルを得る必要があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-20170913-cmsturn

該当製品

修正済みソフトウェア

この脆弱性は、Cisco Meeting Server（CMS）導入環境がリリース 2.0.16、2.1.11、または 2.2.6 より前のリリースの CMS ソフトウェアを実行していて、以下のすべての追加条件を満たしている場合、影響を与えます。

- 導入環境が CMS に組み込まれた TURN サーバを使用している。
- TURN サーバが Transport Layer Security（TLS）接続を使用している。 メインボード管理プロセッサ（MMP）インターフェイスで、TLS プロトコルが TURN サーバで実行されるよう設定されている。
- TURN サーバが他の共存 CMS サービスと同じ仮想マシンで実行されている。
- TURN サーバが Call Bridge、Web ブリッジ、または CMS 導入環境内のデータベース クラスタに含まれるデータベース ノードと同じ仮想マシン上で実行されている。

管理者は CLI の **version** コマンドを使用して、デバイスで実行されている CMS ソフトウェア リリースを判別できます。 次に、CMS ソフトウェア リリース 2.0.6 を実行しているデバイスのコマンド出力例を示します。

```
system> version

2_0_6
```

TURN サーバで TLS を実行するように設定するには、コンフィギュレーションに **turn tls** コマンドと **turn certs** コマンドが存在している必要があります。 TURN サーバの MMP TLS 設定は、管理者が MMP コンソールで **turn** コマンドを発行することにより確認できます。

次に、TURN サーバに TLS が設定されていないシステムでの **turn** コマンドの出力例を示します。

```
cms> turn

Enabled : true
Username : cisco
Password : 1234
Realm : nicedet.com
Public IP : none
Relay address : 1.2.3.4
Listen interface a
```

次に、TURN サーバに TLS が設定されたシステムでの **turn** コマンドの出力例を示します。

```
cms> turn

Enabled : true Username : cisco Password : 1234 Realm : nicedet.com Public IP : none Relay
address : 1.2.3.4 TLS port               : 3479
TLS cert               : turn.crt
TLS key       : turn.key
TLS bundle    : none
Listen interface a
```

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。

シスコは、この脆弱性が次の条件のいずれかを満たす CMS 導入環境には影響しないことを確

認しました。

- 導入環境で TURN サーバを使用していない。
- 導入環境でサードパーティの TURN サーバを使用している。
- TURN サーバが他のサービスと共存しない専用 CMS 上で実行されている。
- TURN サーバで TLS 設定が無効にされている。

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017-September-13

利用規約