

Cisco IOSソフトウェアおよびCisco Unified Communications ManagerのSession Initiation Protocol(SIP)パケット処理におけるメモリリークの脆弱性



アドバイザリーID : Cisco-SA-20111107- [CVE-2011-0941](#)
CVE-2011-0941
初公開日 : 2011-11-07 16:36
バージョン 1.0 : Final
CVSSスコア : [7.8](#)
回避策 : No Workarounds available
Cisco バグ ID : [CSCtj09179](#)

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 IOSソフトウェアおよびCisco Unified Communications Managerには、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、該当ソフトウェアによる不正なパケットの不適切な処理に起因します。 認証されていないリモートの攻撃者は、悪意のあるネットワーク要求をターゲットシステムに送信することで、この脆弱性を不正利用する可能性があります。 これが成功すると、攻撃者によってデバイスが応答しなくなる可能性があり、その結果、DoS状態が発生します。

シスコはこの脆弱性を確認し、ソフトウェアアップデートをリリースしました。

脆弱性を不正利用するには、攻撃者は該当システムに悪意のあるSIPパケットを送信する必要があります。 ほとんどの環境ではSIPを使用して外部接続が制限されているため、攻撃者は攻撃を受ける前に内部ネットワークにアクセスする必要があります。 さらに、音声ネットワークとデータネットワークが分離された環境では、攻撃者が音声トラフィックにサービスを提供するネットワークにアクセスできず、SIPパケットの送信が許可される可能性があり、悪用の難易度がさらに高まります。

シスコはCVSSスコアを通じて、機能的なエクスプロイトコードが存在することを示しています

が、このコードが一般に公開されることは確認されていません。

該当製品

シスコは、[CSCti75128](#)および[CSCtj09179](#)のバグIDのリリースノートを発行しています。

脆弱性のある製品

8.5(1)、8.0(3a)su1、7.1(5b)su3、および6.1(5)su2よりも前のバージョンのCisco Unified Communications Managerには脆弱性が存在します。シスコは、該当するCisco IOSソフトウェアリリースのリストをCisco Bug ID CSCtj09179で公開しています。このアラートの「ベンダーに関する発表」セクションには、Bug IDへのリンクが含まれています。

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。

回避策

適切なアップデートを適用することを推奨します。

管理者は、IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけが該当システムにアクセスできるようにすることを検討できます。

管理者は、SIPを必要としないデバイスでSIP処理を無効にすることを検討できます。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

契約が有効なシスコのお客様は、[Cisco](#)のSoftware Centerからアップデートを入手できます。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)に連絡するか、tac@cisco.comのEメールでアップグレードを入手できます。

推奨事項

```
$propertyAndFields.get("recommendations")
```

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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やその公表を確認していません。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA->

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2011年11月7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。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。