# Cisco Unified Presence Serverのサービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20130227-cups
初公開日 : 2013-02-27 16:00
最終更新日 : 2013-02-28 13:25
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCua89930

CVE-2013-1137

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 Unified Presence Server(CUPS)には、認証されていないリモートの攻撃者が該当デバイスにサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が存在します。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ています。この脆弱性を軽減する回避策があります。このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130227-cups

## 該当製品

### 脆弱性のある製品

次の製品は、このアドバイザリに記載されている脆弱性の影響を受けます。

- Cisco Unified Presence Server 8.6
- Cisco Unified Communications Manager IM and PresenceサービスVer.9.0

### 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 Unified Presenceは、組織内および組織間で最も効果的な方法で人々を結び付ける、標準ベースのエンタープライズプラットフォームです。このオープンで拡張可能なプラットフォームに

より、Cisco Unified Communicationsとその他のアプリケーション間で、プレゼンスおよびインスタントメッセージング(IM)情報のセキュアな交換が促進されます。

DoS脆弱性

Cisco Unified Presence Server(CUPS)には、認証されていないリモートの攻撃者が該当デバイスにDoS状態を引き起こす可能性のある脆弱性が存在します。攻撃者は、巧妙に細工されたパケットをSession Initiation Protocol(SIP)ポート（TCPポート5060）に送信することで、この問題を不正利用する可能性があります。その結果、CPU使用率が増加し、サービスの中断につながる可能性があります。この脆弱性は、Cisco Bug ID CSCua89930( 登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-1137が割り当てられています。

## 回避策

TCPポート5060で信頼できない送信元からのトラフィックをフィルタリングすることで、この脆弱性を回避できます。

## 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場合は、 http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の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。

修正は、cisco.comのソフトウェアダウンロードセンターから入手できます。このダウンロードセンターには、次のリンクからアクセスできます。

http://software.cisco.com/download/navigator.html

| Cisco Unified Presence Serverのバージョン | 推奨リリー |
|---|---|
| 8.6 | 8.6.4SU2 |
| 9.0 | 9.1.1 |

修正済みバージョンは、バージョン8.6では8.6.4SU2、バージョン9.0では9.1.1です。 バージョン9.1には脆弱性はありません。

注：バージョン9.0のアップグレードパスは、上記のリンクから入手可能なバージョン9.1.1です。

## 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。

この脆弱性は、シスコの社内テストで発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130227-cups

## 改訂履歴

| | | |
|---|---|---|
| リビジョン 1.1 | 2013年2月28日 | 該当バージョンと修正済みバージョンを修正 |
| リビジョン 1.0 | 2013年2月27日 | 初回公開リリース |

## 利用規約

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。