Cisco Unified Communications Manager IM and PresenceサービスにおけるDoS脆弱性

アドバイザリーID : cisco-sa-20130821-cup [CVE-2013-3453]
初公開日 : 2013-08-21 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCud84959

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 Communications Manager IM and Presence Service(CUCM)にはサービス拒否(DoS)の脆弱性があり、認証されていないリモートの攻撃者によってサービス拒否(DoS)状態が引き起こされる可能性があります。この脆弱性が不正利用されると、プレゼンスサービスの中断が引き起こされ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ています。

この脆弱性の不正利用を軽減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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130821-cup

該当製品

脆弱性のある製品

Cisco Unified Communications Manager IM and Presence Serviceの9.1(2)より前のすべてのバージョンが、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ソフトウェアバージョンの確認

実行中のCisco Unified Presenceソフトウェアのバージョンを確認するには、コマンドラインインターフェイスから show version activeコマンドを発行します。

次の例は、Cisco Unified Presenceソフトウェアバージョン8.6.0を示しています。

```
admin: show version active
Active Master Version: 8.6.0.97041-43
```

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 Communications Manager IM and Presence ServiceおよびCisco Unified Presence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。

この脆弱性は、メモリリークに起因します。攻撃者は、ポート5060または5061に対して大量のTCP接続を生成することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は該当デバイスにDoS状態を引き起こす可能性があります。この状態を解消するには、サーバを再起動する必要があります。

この脆弱性は、Cisco Bug ID CSCud84959(登録ユーザ専用)として文書化され、Common Vulnerabilities Enumerator(CVE)IDとしてCVE-2013-3453が割り当てられています。

回避策

この脆弱性を軽減する回避策はありません。

ネットワーク内のCiscoデバイスに適用可能な他の対応策は、このアドバイザリに関連するCisco適用対応策速報を次のリンク先で参照できます。
https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=30393

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。

Cisco Unified Communications Manager IM and Presenceサー	推奨リリー

ビスのバージョン	ス
8.6(x)	8.6(5)SU1
9.0(x)、9.1(x)	9.1(2)*

*注：Cisco Unified Communications Manager IM and Presence Service 9.1(2)は、2013年9月中旬にリリースされる予定です。

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。

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。

このアドバイザリで説明されている脆弱性は、シスコの社内テストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130821-cup

改訂履歴

リビジョン 1.0	2013年8月21日	初版リリース

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。