Cisco TelePresence Supervisor MSE 8050のDoS脆弱性

アドバイザリーID : cisco-sa-20130515-mse CVE-2013-1236
初公開日 : 2013-05-15 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 : CSCuf76076 CSCuf79763

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 TelePresence Supervisor MSE 8050には脆弱性があり、認証されていないリモートの攻撃者がCPUの高使用率と該当システムのリロードを引き起こす可能性があります。

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。これらの脆弱性に対しては回避策がありません。

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-20130515-mse

該当製品

脆弱性のある製品

ソフトウェアバージョン2.2(1.17)以前を実行しているCisco TelePresence Supervisor MSE 8050は、この脆弱性の影響を受けます。

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。

詳細

Cisco TelePresence MSE 8000シリーズは、高解像度ビデオ会議および音声通信用のシャーシベースのプラットフォームです。Cisco TelePresence Supervisor MSE 8050は、Cisco TelePresence MSE 8000シリーズの中核であり、Cisco TelePresence MSE 8000シリーズの一部

としてサポートされるシャーシおよびその他のCisco TelePresence製品の管理サービスを提供します。

Cisco TelePresence MSE 8050スーパーバイザのネットワークスタックにおける脆弱性により、認証されていないリモートの攻撃者がCPUの高使用率と該当システムのリロードを引き起こす可能性があります。

この脆弱性は、大量に送信されるTCP接続要求の不適切な処理に起因します。攻撃者は、一連のTCPセグメントを該当システムの管理IPアドレスに高頻度で送信することで、この脆弱性を不正利用する可能性があります。 この脆弱性を不正利用するには、完全なTCP 3ウェイハンドシェイクが必要です。この不正利用により、攻撃者はCPUの高使用率を引き起こし、該当システムのリロードを引き起こし、サービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、Cisco Bug ID CSCuf76076(登録ユーザ専用)および CSCuf79763(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposure(CVE)IDとしてCVE-2013-1236が割り当てられています。

回避策

これらの脆弱性に対しては回避策がありません。

修正済みソフトウェア

この脆弱性は、Cisco TelePresence Supervisor MSE 8050ソフトウェアバージョン2.3(1.31)以降で解決されています。

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。

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-20130515-mse

改訂履歴

リビジョン 1.0	2013年5月15日	初回公開リリース

利用規約

本アドバイザリ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。 本アドバイザリ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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、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。