Cisco Prime Central for Hosted Collaboration Solution Assuranceの過剰なCPU使用率の脆弱性

アドバイザリーID : cisco-sa-20130227-hcs CVE-2013-1135
初公開日 : 2013-02-27 16:00
バージョン 1.0 : Final
CVSSスコア : 7.1
回避策 : No Workarounds available
Cisco バグ ID : CSCuc07155

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 Prime Central for Hosted Collaboration Solution(HCS)Assurance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。この脆弱性が不正利用されると、音声サービスのモニタリングが中断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-hcs

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 Prime Central for HCS Assurance 8.6
- Cisco Prime Central for HCS Assurance 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 Prime Central for HCS Assuranceは、シスコのパートナーが加入者ベースのソリューションとして幅広いシスココラボレーションアプリケーションをお客様に提供できるサービスです。

不正なTLSメッセージによるサービス妨害(DoS):

Cisco Prime Central for HCS Assuranceバージョン8.6および9.0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を過度に消費することでDoS状態を引き起こす可能性があります。

この脆弱性は、システムが受信した不正なTLSメッセージによって引き起こされます。攻撃者は、不正なTLSメッセージをTCPポート9043またはTCPポート9443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。この脆弱性の不正利用に成功すると、攻撃者は使用可能なすべてのCPUサイクルを消費し、音声サービスのモニタリングを中断する可能性があります。この脆弱性は、Cisco Bug ID CSCuc07155(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2013-1135が割り当てられています。

回避策

この脆弱性に対する回避策はありません。

ネットワーク内のシスコデバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Intelligence』にて参照できます。

https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=28034

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 Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける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 Prime Central for HCS Assuranceバージョン	推奨リリー
8.x	9.1(1)
9.0	9.1(1)

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-20130227-hcs

改訂履歴

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。