Cisco Prime Central for Hosted Collaboration Solution Assurance Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20130821-hcm

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130821-hcm

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。

Revision 1.0

For Public Release 2013 August 21 16:00 UTC (GMT)

目次

要約

Cisco Prime Central for Hosted Collaboration Solution（HCS）Assurance には複数の脆弱性があり、認証されていないリモートの攻撃者がサービス拒否（DoS）状態を引き起こす可能性があります。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、システム リソースの不足を招く可能性があります。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130821-hcm

該当製品

脆弱性が認められる製品

次の製品は、このアドバイザリに記載され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
- Cisco Prime Central for HCS Assurance 9.1

脆弱性が認められない製品

他のシスコ製品においてこの脆弱性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（旧名称：Cisco Hosted Collaboration Mediation（HCM））は、シスコ パートナーがサブスクライバ ベースのソリューションとしてさまざまなシスコ コラボレーション アプリケーションを顧客に提供するためのサービスです。

Cisco Prime Central for HCS Assurance には複数の脆弱性があり、認証されていないリモートの攻撃者が TCP 接続をフラッディングさせてサービスを中断させ、該当システムを DoS 状態にする可能性があります。

メモリ リークの脆弱性

Cisco Prime Central for HCS Assurance にはメモリ リークの脆弱性があり、認証されていないリモートの攻撃者が脆弱な TCP ポートに継続的なフラッディング攻撃を仕掛けて、該当システムを DoS 状態に陥らせる可能性があります。この脆弱性は、Cisco Bug ID CSCub59158（登録ユーザのみ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-3390 が割り当てられています。この状態をクリアするには、サーバを再起動する必要があります。Cisco Hosted Collaboration Mediation Service Assurance 9.1 以前のバージョンが影響を受けます。

メモリ枯渇の脆弱性

Cisco Prime Central for HCS Assurance にはメモリ枯渇の脆弱性が 2 つあり、認証されていないリモートの攻撃者が当該システムに対して TCP 接続の継続的なフラッディング攻撃を仕掛ける可能性があります。当該システムに対する TCP 接続のフラッディングが継続されると、メモリが枯渇し、Web のグラフィカル ユーザ インターフェイスにアクセスできなくなったり、基本コマンドの実行時にメモリ不足のエラーが生じることになります。

1 つ目の脆弱性は、Cisco Bug ID CSCtz90114（登録ユーザのみ）として文書化され、CVE ID として CVE-2013-3389 が割り当てられています。この脆弱性の影響を受けるのは、TCP ポート 61615 と 61616 です。Cisco Hosted Collaboration Mediation Service Assurance 9.1 以前のバージョンが影響を受けます。

2 つ目の脆弱性は、Cisco Bug ID CSCtz92776（登録ユーザのみ）として文書化され、CVE ID として CVE-2013-3388 が割り当てられています。この脆弱性の影響を受けるのは一時的な Java ポート（44444）です。Cisco Hosted Collaboration Mediation Service Assurance 9.1 以前のバージョンが影響を受けます。

ディスク枯渇の脆弱性

Cisco Prime Central for HCS Assurance にはディスク枯渇の脆弱性があり、認証されていないリモートの攻撃者が該当システムで 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 CSCua42724（登録ユーザ専用）として文書化され、CVE ID として CVE-2013-3387 が割り当てられています。 TCP 接続のフラッディングによって、ディスク領域が使い尽く

されるまでエラー ログが生成されます。この状況から回復するには、ログ ファイルを削除する必要があります。この脆弱性の影響を受けるのは、オムニバス ポート（TCP 5400）です。Cisco Hosted Collaboration Mediation Service Assurance 9.1 以前のバージョンが影響を受けます。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCub59158: Memory Leak After TCP Flood Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtz90114: Prime Central Memory Exhaustion From TCP Flood Calculate the environmental score of					
CVSS Base Score - **7.8**					
Acces	Access	Authentica	Confidenti	Integr	Availabi

s Vecto r	Comple xity	tion	ality Impact	ity Impa ct	lity Impact
Netw ork	Low	None	None	None	Comple te
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtz92776: Memory Exhaustion After TCP Flood Calculate the environmental score of					
CVSS Base Score - **7.8**					
Acces s Vecto r	Access Comple xity	Authentica tion	Confidenti ality Impact	Integr ity Impa ct	Availabi lity Impact
Netw ork	Low	None	None	None	Comple te
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCua42724: Disk Exhaustion From Logging of TCP Flood Calculate the environmental score of					
CVSS Base Score - **7.8**					
Acces s Vecto r	Access Comple xity	Authentica tion	Confidenti ality Impact	Integr ity Impa ct	Availabi lity Impact
Netw ork	Low	None	None	None	Comple te
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

本アドバイザリに記載された脆弱性が不正利用された場合、リモートの攻撃によって、サービス

中断の原因となるメモリ リークや DoS 状態が引き起こされる可能性があります。

ソフトウェア バージョンおよび修正

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, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード ソリューションを確認してください。

Cisco Prime Central for HCS Assurance Version	Recommended Release
8.x	9.2(1)
9.x	9.2(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、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。

回避策

これらの脆弱性の回避策はありません。

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレード ソフトウェアを入手できます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組

織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

多言語による各地の電話番号、説明、E メール アドレスなどの TAC の連絡先情報については、Cisco Worldwide Contact を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、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とその公表は確認しておりません。

これらの脆弱性は、シスコの社内テストで発見されたものです。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130821-hcm

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E

メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2013-August-21	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。シスコ セキュリティ アドバイザリについては、すべて http://www.cisco.com/go/psirt/ で確認できます。