Multiple Vulnerabilities in Cisco Prime Collaboration Assurance

Advisory ID: cisco-sa-20150916-pca

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150916-pca

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 2015 September 16 16:00 UTC (GMT)

目次

要約

Cisco Prime Collaboration Assurance ソフトウェアには、次の脆弱性があります。

- Cisco Prime Collaboration Assurance Web Framework Access Controls Bypass Vulnerability
- Cisco Prime Collaboration Assurance Information Disclosure Vulnerability
- Cisco Prime Collaboration Assurance Session ID Privilege Escalation Vulnerability

Cisco Prime Collaboration Assurance Web Framework Access Controls Bypass Vulnerability と Cisco Prime Collaboration Assurance Session ID Privilege Escalation Vulnerability の不正利用に成功した認証された攻撃者は、該当システムによって管理された任意のドメインまたはユーザの管理者特権を使用してタスクを実行できます。

Cisco Prime Collaboration Assurance Information Disclosure Vulnerability の不正利用に成功した認証された攻撃者は、システム データベースにインポートされたデバイスの機密情報（Simple

Network Management Protocol（SNMP）コミュニティ ストリングや管理者クレデンシャルなど）にアクセスできます。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 これらの脆弱性を軽減する回避策はありません。 このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150916-pca

該当製品

脆弱性が存在する製品

Cisco Prime Collaboration Assurance ソフトウェアの脆弱なバージョンを実行している製品は、これらの脆弱性の影響を受けます。

脆弱性が存在しない製品

Cisco Prime Collaboration Provisioning は、このセキュリティ アドバイザリに記載されている脆弱性の影響を受けませんが、別のアクセス制御バイパスの脆弱性が見つかっており、次のリンクにある『*Cisco Prime Collaboration Provisioning Web Framework Access Controls Bypass Vulnerability*』セキュリティ アドバイザリで公開されています。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150916-pcp

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 Collaboration は、ユーザやサービスのプロビジョニングに加えて、Cisco Unified Communications コンポーネントと Cisco TelePresence コンポーネントの迅速なインストールとメンテナンスを可能にします。

Cisco Prime Collaboration Assurance Web Framework Access Controls Bypass Vulnerability

Cisco Prime Collaboration Assurance の Web フレームワークの脆弱性を不正利用すれば、認証されたリモート攻撃者による高度な特権機能へのアクセスができます。

この脆弱性の原因は、認可とアクセス制御の不適切な実装です。 攻撃者は、巧妙に細工された URL をシステムに送信することにより、この脆弱性を不正利用する可能性があります。 攻撃者がこの脆弱性を不正利用するためには、システムにログインする必要があります。

このエクスプロイトを使用すると、攻撃者は、管理者特権を持っているユーザにのみアクセスが許可された一部の機能にアクセスする可能性があります。 この脆弱性を利用して、攻撃者は、追加の管理者ユーザの作成したり、システムがマルチテナント環境で使用されている場合に別のドメインからの情報にアクセスしたりできます。

この脆弱性は、Cisco Bug ID CSCus62671（登録ユーザ専用）、および CSCus62652（登録ユーザ専用）として文書化され、Common Vulnerabilities and Exposures（CVE）ID CVE-2015-4304 が割り当てられています。

Cisco Prime Collaboration Assurance Information Disclosure Vulnerability

Cisco Prime Collaboration Assurance の Web フレームワークの脆弱性を不正利用すれば、認証さ

れたリモート攻撃者によるシステム データベースにインポートされたデバイスに関する情報へのアクセスができます。

この脆弱性の原因は、認可とアクセス制御の不適切な実装です。 攻撃者は、巧妙に細工された URL をシステムに送信することにより、この脆弱性を不正利用する可能性があります。 攻撃者がこの脆弱性を不正利用するためには、システムにログインする必要があります。

このエクスプロイトを使用すると、攻撃者は、他の顧客またはドメインのデバイスを含む、システム データベースにインポートされたデバイスに関する情報にアクセスする可能性があります。 攻撃者が取得可能な情報には、SNMP コミュニティ ストリングとデバイス管理者クレデンシャルが含まれます。 これにより、攻撃者は、これらのデバイスへの管理者アクセス権を取得できます。

この脆弱性は、Cisco Bug ID CSCus62656（登録ユーザ専用）と CVE ID CVE-2015-4305 で文書化されています。

Cisco Prime Collaboration Assurance Session ID Privilege Escalation Vulnerability

Cisco Prime Collaboration Assurance の Web フレームワークの脆弱性を不正利用すれば、認証されたリモート攻撃者によるシステムにログインしているユーザに関する情報（ユーザのセッション ID など）へのアクセスができます。

この脆弱性の原因は、認可とアクセス制御の不適切な実装です。 攻撃者は、巧妙に細工された URL をシステムに送信することにより、この脆弱性を不正利用する可能性があります。 攻撃者がこの脆弱性を不正利用するためには、システムにログインする必要があります。

このエクスプロイトを使用すると、攻撃者は、システムにログインしているユーザに関する情報（ユーザのセッション ID など）にアクセスすることができます。 この識別子を使用して、攻撃者は、システムがマルチテナント用に設定されている場合に、任意のドメインまたは顧客の任意のユーザ（管理者ユーザを含む）になりすますことができます。 この情報を使用して、攻撃者は、セッション ID が有効な期間に特権機能を実行することができます。

この脆弱性は、Cisco Bug ID CSCus88343（登録ユーザ専用）と CSCus88334（登録ユーザ専用）、および CVE ID CVE-2015-4306 で文書化されています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、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

CSCus62671 and CSCus62652 - Cisco Prime Collaboration Assurance Web Framework Access Controls Bypass Vulnerability Calculate the environmental score of					
CVSS Base Score - **9.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCus62656 - Cisco Prime Collaboration Assurance Information Disclosure Vulnerability Calculate the environmental score of					
CVSS Base Score - **4.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Partial	None	None
CVSS Temporal Score - **3.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCus88343 and CSCus88334 - Cisco Prime Collaboration Assurance Session ID Privilege Escalation Vulnerability Calculate the environmental score of					
CVSS Base Score - **8.5**					
Acces	Access	Authentica	Confidenti	Integrit	Availabi

s Vecto r	Comple xity	tion	ality Impact	y Impact	lity Impact
Netw ork	Medium	Single	Complete	Compl ete	Comple te
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
High		Official-Fix		Confirmed	

影響

Cisco Prime Collaboration Assurance Web Framework Access Controls Bypass Vulnerability と Cisco Prime Collaboration Assurance Session ID Privilege Escalation Vulnerability の不正利用に成功した認証された攻撃者は、影響を受けるシステムによって管理されたドメインまたは顧客の管理者の特権を使用したタスクを実行できます。

Cisco Prime Collaboration Assurance Information Disclosure Vulnerability の不正利用に成功した認証された攻撃者は、システム データベースにインポートされたデバイスの機密情報（SNMP コミュニティ ストリングや管理者クレデンシャルなど）にアクセスできます。

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 Alerts 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、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。

Cisco Prime Collaboration Assurance Web Framework Access Controls Bypass Vulnerability、Cisco Prime Collaboration Assurance Information Disclosure Vulnerability、および Cisco Prime Collaboration Assurance Session ID Privilege Escalation Vulnerability は、Cisco Prime Collaboration Assurance ソフトウェア リリース 10.5.1 MSP パッチ *cpc-assurance-patchbundle-10.5.1.53684-1.x86_64.tar.gz* とリリース 11.0 以降で修正されています。 現時点で、Cisco Prime Collaboration Assurance ソフトウェア リリース 10.6 またはリリース 10.5 ENT の修正済みリリースは存在しません。

回避策

これらの脆弱性を軽減する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 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 からソフトウェア パッチおよびバグ フィックスを入手することができます。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、シスコ認定パートナー、リセラー、およびディストリビュータ（認定サードパーティ 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）に連絡してソフトウェア パッチおよびバグ フィックスを入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

ソフトウェア パッチまたはバグ フィックス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 にソフトウェア パッチまたはバグ フィックスを要求してください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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、サポート ケースの解決中にシスコに報告されました。

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 に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150916-pca

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
- fulldisclosure@seclists.org

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。

今後のドキュメントや関連コンテンツの入手手順については、Security Vulnerability Policy の Receiving Security Vulnerability Information from Cisco を参照してください。

更新履歴

Revision 1.0	2015-September-16	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/web/about/security/psirt/security_vulnerability_policy.html を参照してください。 この Web ページには、Cisco Security Advisory 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。 すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。

Cisco Security Advisories
Cisco Intrusion Prevention System Signatures
Cisco Applied Mitigation Bulletins
Cisco Security Blog
Cisco Event Response Pages
Cisco IntelliShield Alerts
Cisco Security Notices
Cisco Security Responses
Cisco Cyber Risk Reports
Cisco Security White Papers
Snort Rules