Cisco Prime Collaborationプロビジョニング Webフレームワークのアクセスコントロールバイパスの脆弱性

アドバイザリーID : cisco-sa-20150916-pcp CVE-2015-4307
初公開日 : 2015-09-16 16:00
バージョン 1.0 : Final
CVSSスコア : 8.5
回避策 : No Workarounds available
Cisco バグ ID : CSCut64111

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 Collaborationプロビジョニング(PCP)のWebフレームワークの脆弱性により、認証されたリモートの攻撃者がより高い権限を持つ機能にアクセスできる可能性があります。

この不正利用により、攻撃者は機能にアクセスできる可能性があります。一部の機能には、管理者権限を持つユーザのみがアクセスできる必要があります。これには、管理ユーザの作成が含まれます。

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-20150916-pcp

該当製品

脆弱性のある製品

脆弱性のあるバージョンのCisco Prime Collaboration Provisioningソフトウェアを実行している製品は、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

Cisco Prime Collaboration Assuranceはこの脆弱性の影響を受けません。ただし、Cisco Prime Collaboration Assuranceには、別のアクセスコントロールバイパスの脆弱性が発見されています。この脆弱性は、次のリンクの『 Multiple Vulnerabilities in Cisco Prime Collaboration

Assurance』セキュリティアドバイザリで公開されています。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150916-pca

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、Cisco Unified Communicationsおよび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、およびユーザとサービスのプロビジョニングを可能にします。

Cisco Prime Collaborationプロビジョニング(PCP)のWebフレームワークの脆弱性により、認証されたリモートの攻撃者がより高い権限を持つ機能にアクセスできる可能性があります。

この脆弱性は、許可およびアクセス制御の不適切な実装に起因します。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で、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には、システムにログインする必要があります。

この不正利用により、攻撃者は機能にアクセスできる可能性があります。一部の機能には、管理者権限を持つユーザのみがアクセスできる必要があります。この脆弱性により、攻撃者は追加の管理ユーザを作成し、データにアクセスしたりデータを操作したりできる可能性があります。

この脆弱性は、Cisco Bug ID CSCut64111(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-2015-4307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。

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, 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、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。

この脆弱性は、Cisco Prime Collaborationプロビジョニングソフトウェアリリース11.0以降で解決されています。

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、シスコ内部でのセキュリティテストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150916-pcp

改訂履歴

リビジョン 1.0	2015年9月16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。