Cisco Unityでの認証バイパス

Medium

アドバイザリーID : cisco-sa-20081008-unity
初公開日 : 2008-10-08 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2008-3814

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 Unityには脆弱性があり、認証されていないユーザがCisco Unityサーバの設定パラメータの一部を表示または変更でき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。この脆弱性に対しては回避策があります。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20081008-unity で公開されています。

該当製品

Cisco Unityは、音声およびユニファイドメッセージングプラットフォームです。Cisco Unityは、Microsoft ExchangeまたはIBM Lotus Dominoと相互運用できるように設定できます。これにより、ユーザは単一の受信トレイから電子メール、音声、およびファックスメッセージにアクセスできます。

脆弱性のある製品

すべてのCisco Unityバージョン4.x、5.x、および7.xが、この脆弱性の影響を受ける可能性があります。

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 Unityサーバが匿名認証用に設定されている場合、認証バイパスの影響を受ける可能性があ

ります。匿名認証は、Cisco UnityサーバがMicrosoft Windows（統合Windows認証）ではなくサブスクライバに対して認証される場合に使用されます。デフォルトでは、管理者が統合Windows認証方式を認証に使用するようにCisco Unityが設定されています。

認証メカニズムの詳細については、『Cisco Unity Administratorで使用可能な認証方式』セクションの「Cisco Unityのインストールガイド」を参照してください。

この認証バイパスの脆弱性により、認証されていないユーザが一部のシステム設定パラメータを表示または変更できるようになります。この脆弱性の不正利用によって資格情報、個人を特定できる情報、またはユーザ情報を取得することはできません。

この脆弱性は、Cisco Bug ID CSCsr86943 (登録ユーザ専用)として文書化され、Common Vulnerability and Exposures(CVE)IDとしてCVE-2008-3814が割り当てられています。

回避策

統合Windows認証は、この脆弱性の影響を受けず、匿名認証の代わりに使用される可能性があります。

認証メカニズムとその設定方法の詳細については、『Setting Up Authentication for the Cisco Unity Administrator』セクションの「Installation Guide for Cisco Unity」を参照してください。

修正済みソフトウェア

この脆弱性は、4.2.1リリースのCisco Unityソフトウェアバージョン4.2.1ES161、5.xリリースの5.0ES53、および7.xリリースの7.0ES8で修正されています。

Cisco Unityソフトウェアの最新バージョンは、https://sec.cloudapps.cisco.com/support/downloads/go/Redirect.x?mdfid=274246502からダウンロードできます。各リリースのソフトウェアは、4.2(1) ESリリース、5.0(1) ESリリース、7.0(2) ESリリースで入手できます。

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この脆弱性は、VoIPShield Systems社からシスコに報告されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20081008-unity

改訂履歴

リビジョン 1.0	2008年10月8日	初版リリース

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。