IBMサーバでの音声製品の脆弱性

severity

アドバイザリーID : cisco-sa-20040121-voice

初公開日 : 2004-01-21 17:00

バージョン 1.0 : Final

回避策 : No Workarounds available

Cisco バグ ID :

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

IBMプラットフォームにシスコの音声製品をデフォルトでインストールすると、Director Agentが安全でない状態でインストールされ、Directorサービスはリモート管理制御やDenial of Service(DoS)攻撃に対して脆弱になります。この脆弱性は設定を変更することで軽減できます。シスコは、脆弱性のあるポートを閉じ、Directorエージェントをアップグレードせずにセキュアな状態にする修復スクリプトを提供しています。

このアドバイザリは次のURLで入手できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040121-voice

該当製品

脆弱性のある製品

デフォルト設定でインストールされたIBMサーバで実行されているCisco音声製品は、TCPまたはUDPポート14247を開いたままにしておくと影響を受けます。この脆弱性を確認するには、管理者がサーバでコマンドウィンドウを開き、**netstat -a**と入力します。ポート14247がリストされている場合、サーバはリモート管理制御およびDenial of Service(DoS)攻撃に対して脆弱です。

該当するシスコの音声製品：

- Cisco CallManager
- Cisco IP Interactive Voice Response(IP IVR)
- Cisco IP Call Center Express(IPCC Express)

- Cisco Personal Assistant（PA）
- Cisco Emergency Responder（CER）[CiscoEmergencyResponderCER]
- Cisco Conference Connection（CCC）
- 該当するOSバージョンのIBMで実行されているCisco Internet Service Node(ISN)。

該当するIBMベースのサーバモデル番号：

- IBM X330（8654または8674）
- IBM X340
- IBM X342
- IBM X345
- MCS-7815-1000
- MCS-7815I-2.0
- MCS-7835I-2.4
- MCS-7835I-3.0

該当するOSバージョン：

OS 2000.2.6より前のIBMサーバ上で実行されているすべてのオペレーティングシステム(OS)バージョン。この通知の日付ではまだリリースされていません。

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

IBMサーバ上のCisco音声製品のデフォルトのインストールでは、IBM Directorは非セキュア状態でインストールされ、TCPポートとUDPポートは開かれたままになりま14247。すべてのDirector Server/Consoleエージェントは、ポート14247を介して接続し、認証を必要とせずに管理レベルの制御を行うことができます。また、ネットワークセキュリティスキャナスキャンポート14247により、IBM Directorエージェントプロセスtwgipc.exeがトリガーされ、サーバがリブートされるまでCPUの100 %が使用される可能性があります。これらの脆弱性は、2つのCisco Bug ID

- **CSCed33037**:IBM Directorエージェトデフォルトのインストールではリモートアクセスが可能です。
- **CSCed23357**:Director 22または3.11を搭載したIBMサーバはDoSに対して脆弱です。

回避策

シスコの修復スクリプトにより、ディレクタエージェントに次の3つのレベルのセキュリティが追加されます。

1. Directorエージェントは、Directorサーバからのリモート接続をTCPポート14247またはUDPポートでリッスンしなくなりました。この変更により、「影響」セクションで説明されているDenial of Service(DoS)攻撃が防止されます。

2. 修復スクリプトは、ポート14247が再び有効になった場合でも、Directorエージェントが Directorサーバからの接続を受け入れないように、Directorエージェントを保護します。
3. プログラムの機能には必要ないが、高レベルのアクセスまたは制御を提供するディレクタエージェント実行可能ファイルは、この修復スクリプトによって完全に無効にされます。

注：IBM Directorサーバとコンソールを使用してCisco音声製品を監視している場合、この修復スクリプトによってこれらのIBMサーバへの接続が無効になります。Directorエージェントは、バージョン3.11のポップアップ警告とイベントビューアメッセージ、およびCiscoWorks IP Telephony Monitorなどのネットワーク管理ソフトウェアへのSNMPトラップを引き続き提供します。IBM Director Serverの監視機能を回復するには、OSバージョン2000.2.6でIBM Directorエージェント4.11をリリースする予定です。OSバージョン2000.2.6にアップグレードした後で、Director Serverのサポートを再度有効にできます。

修正済みソフトウェア

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。

これらの脆弱性はIBMサーバ上のCisco音声製品に固有であり、このアドバイザリに記載されているすべての脆弱性は、アップグレードを必要とせずに修復スクリプトで軽減できます。

修復スクリプトは次の場所で入手できます。

http://www.cisco.com/pcgi-bin/tablebuild.pl/cmva-3des

不正利用事例と公式発表

Cisco 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やその公表は確認しておりません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040121-voice

改訂履歴

リビジョン	2004年1月21日	初回公開リリース

1.0		

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。