H.323 メッセージ 処理の脆弱性

severity	**アドバイザリーID :** cisco-sa-20040113-h323 **初公開日 :** 2004-01-13 12:00 **バージョン 1.4 :** Final **回避策 :** Yes **Cisco バグ ID :**	CVE-2004-0056 CVE-2004-0054 CVE-2004-0097 CVE-2003-0819

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

複数のシスコ製品は Voice over Internet Protocol （ VoIP ）かマルチメディアアプリケ– ションで一般的に使用される H.323 メッセージの処理で脆弱性が含まれています。 テスト スイートは University of Oulu によってこのプロトコルを目標とし、脆弱性を識別するために開発されました。

H.323 プロトコルのために導入されました Cisco IOSÂ® ソフトウェア リリース 11.3T でサポートして下さい。 ソフトウェアが音声/マルチメディアアプリケ– ションのためのサポートが含まれている場合リリース 11.3T、およびすべてのより遅い Cisco IOS リリースは影響を受けるかもしれません。 脆弱 な デバイスは IOS ネットワーク アドレス変換（ NAT ）のために設定されるネットワーク要素、またネットワーク要素および IOS Firewall のために設定されるそれらとして H.323 のためのソフトウェアサポートが含まれているデバイスが含まれています（ 別名コンテキストベースのアクセス コントロール（ CBAC ） [CBAC] ）。

Cisco IOS を実行しない他の Cisco 音声 製品はまた影響を受けるかもしれません。

これらの脆弱性がサービス拒否 （ DoS ）を生成 するのに繰り返し不正利用することができます。

このアドバイザリは 113-h323 で利用できます。

該当製品

修正済みソフトウェア

Cisco IOSソフトウェアおよびサポート H.323 パケット処理を実行するすべてのシスコ製品は影響を受けています。 これはこれらのプロトコルのためのサポートが H.323 のためのサポートを有効に することができるのでセッション開始プロトコル（SIP）かメディア ゲートウェイ コントロール プロトコル（MGCP）のために設定されるデバイスを含むかもしれません。 設定 される " Plus " 機能の Cisco IOSイメージは H.323 を不具合が理由で設定に関係なく脆弱デフォルトで有効に するかもしれ、プロトコルが消えないようにしません。

Cisco IOSソフトウェアを実行しない他の該当製品は下記のものを含んでいます:

- Cisco CallManagerバージョン 3.0 ～ 3.3
- Cisco Conference Connection（CCC）
- Cisco Internet Service Node（ISN）
- Cisco BTS 10200 Softswitch
- Cisco 7905 IP Phone H.323 ソフトウェア バージョン 1.00
- バージョンと H.323/SIP ロードを先に実行する Cisco ATA 18x シリーズ 製品より 2.16.1

注: Cisco ATA 18x シリーズ 製品は H.323 のために設定されたときだけ脆弱です。 それらは SIP のために設定されたとき脆弱ではないです。

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、**show version** コマンドを発行してシステム バナーを表示します。 Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。 出力次の行で、イメージ名は「バージョンに」先行しているかっこと IOSリリース名の間で表示する。 その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

次の例は C2500-IS-L のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.0(3)を実行する Cisco製品を指定したものです。 リリース トレイン ラベルは 12.0 です。

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

次の例は C2600-JS-MZ のイメージ名と Cisco IOS ソフトウェア リリース 12.0(2a)T1 を実行する製品を示したものです。

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Cisco IOSバージョン指名についてのその他の情報は http://www.cisco.com/warp/public/620/1.html で利用できます。

Cisco IOSバージョン 10.x を実行する場合、11.1、11.2 またはそれ以前、影響を受けていません。

H.323 トラフィックの Cisco IOS 処理

IOS が H.323 不正 なパケットに脆弱の場合もある 3 つのエリアがあります。 ルータが影響を

受けていたかどうか確認するために以降のセクションを読んで下さい。 TAC ケースをオープンする必要がある場合ケース解決を促進するために推奨される 識別ステップの出力をキャプチャして下さい。

注: H.323 トラフィックはルータを入力することを防ぐためにアクセス リストを使用して H.323 トラフィックをブロックすることを選択すれば、このアドバイザリに記載される脆弱性からデバイスを保護し、下記に記載されていた詳細はあなたに適用しません。 これをする方法の回避策 セクションを詳細については参照して下さい。 Cisco は適切な IOSイメージにことを顧客 アップグレードなるべく早く推奨します。

Cisco IOSソフトウェアが H.323 トラフィックを処理すること Cisco IOSデバイスが H.323 トラフィックを処理して、可能性のある 脆弱であるかどうか確認するために、3 つのさまざまな方法を知っていることは必要です。

1. **H.323 エンドポイント**

これには設定されないで H.323 プロセスをデフォルトで実行するかもしれないプロキシ、またリリースの H.323 ゲートウェイ、H.323 ゲートキーパーおよび H.323 ゲートキーパーが含まれています。 デバイスが影響を受けていたかどうか確認し次のステップと続けて下さい。

イネーブル プロンプトから、**show process CPU コマンドを**実行し、CCH323_CT と呼ばれるプロセスを探して下さい。 Cisco IOSソフトウェアの以降のバージョンでは、**show process CPU を**実行できます **| CCH323 を含んで下さい**。

```
Router# show process cpu | include CCH323
 112 Mwe 60F3E5E0       295112     239401    123220072/24000  0 CCH323_CT
```

注: 設定 される " Plus " 機能のイメージだけ（IP PLUS、ENTERPRISE PLUS のような）音声をサポートし、CCH323_CT プロセスが実行があります。 12.0 に、設定 される " Plus " 機能に 2600 および 3600 のプラットフォームの CCH323_CT プロセスが実行がデフォルトであります。 12.1 に開始して、プロセスは音声カードか DSP カードを挿入してもらう場合デフォルトで動作します。

- CCH323_CT と呼ばれるプロセスを見る場合ルータは影響を受けています。 どのバージョンがデバイスのために適切であるか判別するために IOS 表を参照して下さい。 すぐにアップグレードできない場合次の回避策はあなたのためにはたらくかもしれません
  -ネットワーク内の H.323 を使用していなければ、TCPポート 1720 をブロックするインバウンドアクセスリストはルータを保護しますが、実行可能であるとすぐアップグレードすることが推奨されます。
  - H.323 を使用していれば、既知の、信頼された IP アドレスに TCPポート 1720 トラフィックを制限するためにアクセス リストを設定できます。 再度実行可能であるとすぐ、アップグレードは推奨されます。
- CCH323_CT プロセスを見ない場合、まだ脆弱かもしれません。 H.323 ゲートキーパーのコンフィギュレーションは脆弱です。 影響を受けたコンフィギュレーションは H.323 プロキシのために設定されるそれらのゲートキーパーです。 ゲートキーパーで設定されるか

どうか確認するために、行があるように設定を「グローバルコンフィギュレーションのプロキシ h323" 確認して下さい。「設定されるプロキシ h323" がある場合脆弱です。
- GK プロキシ 機能を使用していなければ、次の設定をすることによってプロキシ 機能をディセーブルにすることができます。
注: これはゲートキーパーが管理するすべての呼び出しを廃棄します。 安全にゲートキーパー機能性を停止できるときだけこれを行って下さい。
```
Router(config)#no proxy h323
Router(config)#gatekeeper
Router(config-gk)#shutdown
Router(config-gk)#no shutdown
```
- H.323 プロキシを使用していれば、オプションはに設定します TCPポート 1720 トラフィックを既知の、信頼された IP アドレスに制限するか、または IOSバージョンをアップグレードするためにアクセス リストをあります。

2. IOS Firewall（コンテキストベースのアクセス コントロール（CBAC））

IOS Firewall（IOS FW 使用するために IOSデバイスがまたはコンテキストベースのアクセス コントロール（CBAC）[CBAC]）設定されれば、**すべての**コマンドことを IOS FW がデバイスで**提示 ip inspect の**発行によって動作しているかどうか見るチェック。 IOS FW がインターフェイスに適用されることを示す次の行を探して下さい。 この場合、FastEthernet0/0 をインターフェイスさせるインスペクション ルール「<NAME>」は応用受信です。

```
Router(config)#no proxy h323
Router(config)#gatekeeper
Router(config-gk)#shutdown
Router(config-gk)#no shutdown
```

- インターフェイス FastEthernet0/0 の受信 IOS FW（CBAC）を消すために、インターフェイス設定モードで次のコマンドを入力して下さい。
```
Router#config t
Router(config)#Interface FastEthernet 0/0
Router(config-if)#no ip inspect <NAME> in
```
- 発信 IOS FW（CBAC）が FastEthernet0/0 で設定される場合、インターフェイス設定モードで次のコマンドを入力して下さい。
```
Router#config t
Router(config)#Interface FastEthernet 0/0
Router(config-if)#no ip inspect <NAME> out
```
- 他の IOS FW 動作を変化しない残して間、だけ H.323 メッセージの IOS FW（CBAC）処理を消すために、グローバル コンフィギュレーション モードで次のコマンドを入力します。
```
Router(config)#no ip inspect name <NAME> h323
```

Cisco は IOS をできるだけ早くアップグレードすることを推奨します。

3. IOS ネットワーク アドレス変換（NAT）

あらゆるインターフェイスでアクティブになる NAT ルールを設定し、NAT がある場合 NAT がデバイスで **show ip nat statistics コマンドのことを**発行によって設定され、アクティブになるかどうか確認して下さい。

```
Router#show ip nat statistics

Total active translations: 3 (3 static, 0 dynamic; 0 extended
```

```
Outside interfaces
Inside interfaces
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

- 出力がないかまたは出力が内部 または 外部 インターフェイス (次 上述の例) をリストしなかったものではなく、IOSデバイスは NAT をしなくて、NAT が理由で脆弱ではないです。
- 出力が内部 または 外部 インターフェイスをリストしたもので場合、NAT が理由で脆弱かもしれません。 次に例を示します。

```
Router#show ip nat statistics

Total active translations: 3 (3 static, 0 dynamic; 0 extended
Outside interfaces
Inside interfaces
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

- 設定がポート アドレス変換 (PAT) 文だけが含まれ、PAT 文が明示的に PAT 変換の TCPポート 1720 を規定 しなければ場合 NAT が理由で脆弱ではないです。
  - PAT だけしているかどうか見るために、IOS NAT 設定は**過負荷**、**ルート マップ**、または**拡張可能な**キーワードなしでの次の NAT ルールが含まれているかどうか確認して下さい。

```
Router#show ip nat statistics

Total active translations: 3 (3 static, 0 dynamic; 0 extended
Outside interfaces
Inside interfaces
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

過負荷、**ルート マップ**、または**拡張可能な**キーワードなしで上記のいずれかの行を見れば、脆弱です。

- H.323 のためのスタティックPAT をしているかどうか見るため (1720) TCPポートは、次のパターンの行を探します。

```
Router#show ip nat statistics

Total active translations: 3 (3 static, 0 dynamic; 0 extended
Outside interfaces
Inside interfaces
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

次の例は脆弱です。

```
Router#show ip nat statistics

Total active translations: 3 (3 static, 0 dynamic; 0 extended
Outside interfaces
Inside interfaces
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

次の例は脆弱ではないです。

```
Router#show ip nat statistics

Total active translations: 3 (3 static, 0 dynamic; 0 extended
Outside interfaces
Inside interfaces
Hits: 0  Misses: 0
```

```
Expired translations: 0
```

`Dynamic mappings:`設定行のうちのどれかが脆弱である場合、回避策 セクションを参照して下さい。

特定の Cisco IOS リリースが脆弱だったかどうか確認するために、製品が影響を受けたソフトウェアのバージョンを実行したかどうか確認するためにソフトウェア バージョン および 修正 セクションで下記のリストを参照して下さい。

脆弱性を含んでいないことが確認された製品

シスコ製品の次のリストは顧客がまたこれらの脆弱性に関して約かかわることができることそれらの製品をリストするためにとりわけ提供されます。 製品は下記の脆弱ではないか、または H.323 処理をサポートしないので影響を受けません。 その他のCisco製品がこれらの脆弱性から影響を受けるために知られていないので脆弱として下記のリストから識別された同様に脆弱ではなかったし、または考慮する必要がある省略されなかったその他のCisco製品。

- Cisco IP Phone モデル 7960、7940、7912、7910、7902、30VIP および 12SP+
- Cisco uOne（すべてのバージョン）
- VG248 Analog Phone Gateway
- Cisco Unity サーバ
- Catalyst 6000 WS-X6608 音声 サービス モジュールおよび WS-X6624 FXS Analog Station Interface モジュール
- PGW2200、SC2200、VSC3000 および H.323 シグナル インターフェイス（彼の）
- Cisco IP/VC 3500 シリーズ
- IP/TV シリーズ
- Catalyst 19xx、28xx、290x、292x、2948g、3000、3200、3900、4000、4912g および 5000 シリーズ スイッチ
- Catalyst 2900XL、2900XL-LRE、2940、2950、2950-LRE、2955、2970、3500XL、3550、および 3750 シリーズ スイッチ
- Cache Engine シリーズ
- Content Engine シリーズ
- SN5400 シリーズ ストレージ ルータ
- VPN 3000 および VPN 5000 シリーズ VPN コンセントレータ
- 音声インターワーキング サービス モジュール（VISM）
- VCO/4K
- Cisco Secure Intrusion Detection System（NetRanger）アプライアンスおよび IDS モジュール
- BR340、WGB340、AP340、AP350 および BR350 Cisco/Aironet無線 製品
- Cisco Aironet 1100 シリーズ、1200 シリーズおよび 1400 シリーズ 無線製品
- Cisco PIX ファイアウォール
- Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール
- CBOS を実行する Cisco 6xx シリーズ DSL モデム
- Cisco 7xx シリーズ ルータ

- Cisco 12000 シリーズ ルータ
- Cisco 10000 シリーズ ルータ
- 61xx および 62xx シリーズ DSLAM
- Cisco CSS11xxx シリーズ (を含む SSL アクセラレータ)
- LocalDirector
- BPX、IGX、MGX WAN スイッチおよびサービス拡張シェルフ
- Cisco Intelligent Contact Management (ICM)
- Cisco ONS 15XXX プラットフォーム

改訂履歴

リビジョン 1.4	2004-October-08	Cisco ATA18x シリーズ アナログ テレフォニーデバイス記述のための詳細 セクションにバグID を追加しました。 Cisco ATA18x シリーズ アナログ テレフォニーデバイス記述のためのソフトウェア バージョン および 修正 セクションのソフトウェア バージョンを変更しました。
リビジョン 1.3	2004-January-16	**show process CPU** の明白にされた構文 | 「該当製品」セクションに **CCH323** コマンドを**含めて下さい**。
リビジョン 1.2	2004-January-15	「要約」および「該当製品」セクションの該当するリリースの明白にされた性質; 12.2XB、12.0、12.1、12.2B、12.2S および 12.2E のための更新済 IOS software 表; 「回避策」セクションの IPSec-H323.exe への更新済ソフトウェア リンク。
リビジョン 1.1	2004-January-14	「該当製品」セクションの下: 「" Plus " 機能の IOSイメージ」の取り替えられた "AS5xxx シリーズ プラット フォームは 」設定 しました; 「H.323 トラフィックの Cisco IOS」処理で、AS5xxx プラットフォームの取除かれた言及; "H.323 エンドポイントの下の更新済メモ」セクション; 「H.323 トラフィックの Cisco IOS」処理セクションの下の更新済メモ; 12.2XB、12.1E、12.2、および 12.0 のための更新済 IOS software 表; 「12.2(19)" への移行するのすべての参照を「 12.2(19)b" に移行するために変更しました; 「回避策」セクションの下、「 Windowsベース アクセス制御リストの口ーカルで制限するために定義の更新済セクション 信頼できるホストだけからの H.323 トラフィックを」; 「不正利用事例と公式発表の下で」区分して下さい、「NISCC 脆弱性経営陣」との「 UNIRAS」の取り替えられた言及

リビジョン 1.0	2004-January-13	初回公開リリース

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。