Cisco IOSソフトウェア H.323 サービス拒否の脆弱性

High	**アドバイザリーID :** cisco-sa-20100922-h323 **初公開日 :** 2010-09-22 16:00 **最終更新日 :** 2016-01-08 22:42 **バージョン 1.3 :** Final **CVSSスコア :** 7.8 **回避策 :** Yes **Cisco バグ ID :** CSCtc73759 , CSCtd33567	CVE-2010-2829 CVE-2010-2828

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 IOS ® ソフトウェアの H.323 実装は Cisco IOSソフトウェアの脆弱なバージョンを実行しているデバイスのサービス拒否（DoS）条件を引き起こすのにリモートで不正利用されるかもしれない 2 脆弱性が含まれています。

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。 脆弱 な デバイスの H.323 をディセーブルにすること以外これらの脆弱性を軽減する回避策がありません。

このアドバイザリは 922-h323 で掲示されます。

注: 2010 年 9月 22 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 6 Cisco Security Advisory が含まれています。 アドバイザリの 5 つは Cisco IOSソフトウェアの脆弱性に対処し、1 つのアドバイザリは Cisco Unified Communications Manager の脆弱性に対処します。 各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決するリリースを記載しています。 次の URLリストの表は正しい 2010 年 9月 22 日送達されたすべての Cisco IOSソフトウェア脆弱性、またはそれ以前ことリリースします:

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a315.shtml

"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクのパブリケーションを」組み込みました:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

該当製品

修正済みソフトウェア

H.323 メッセージを処理するために設定される影響を受けた Cisco IOS ソフトウェア バージョンを実行している Ciscoデバイスはこれらの脆弱性から影響を受けます。 H.323 はデフォルトで有効に なりません。

Cisco IOSソフトウェア デバイスが H.323 サービスを経営したかどうか確認するために、**show process CPU を**発行して下さい | この例に示すように **H323** コマンドを、**含んで下さい**:

```
Router# show process cpu | include H323
 249       16000           3       5333  0.00%  0.00%  0.00%    0 CCH323_CT
 250           0           1          0  0.00%  0.00%  0.00%    0 CCH323_DNS
Router#
```

前例でプロセス CCH323_CT および CCH323_DNS はデバイスで動作しています; 従って、デバイスは H.323 メッセージを受信しています。 デバイスはこれらのプロセスのうちのどれかが（または類似した）アクティブである場合脆弱です。

注: Cisco IOSデバイスが H.323 メッセージを処理します **dial-peer voice コマンドの**発行によるダイヤル ピアを作成することは H.323 プロセスを開始します。

Cisco 製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、機器にログインし show version コマンドを実行してシステムバナーを表示させます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Cisco 機器では、 show version コマンドがない場合や、表示が異なる場合があります。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

!--- output truncated
```

次の例は C1841-ADVENTERPRISEK9-M 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 12.4(20)T を実行している Cisco製品を指定したものです:

```
Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T,
    RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます:
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

脆弱性を含んでいないことが確認された製品

Cisco IOS XR ソフトウェアは、これらの脆弱性の影響を受けません。

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。

改訂履歴

Version	Description	Section	Status	Date
1.3	リンクをバンドル ページにアップデートし、EOL SRND にリンクを取除きました。	概要、回避策	Final	2016-January-08
1.2	12.2SRD が脆弱および first fixed in 12.2SRE であること、そして 12.2SRC が脆弱、first fixed in 12.2SRE であること、こと 12.2SRE が first fixed in 12.2(33)SRE1 である示す修正されたソフトウェア バージョン および 修正。		Final	2011-March-10
1.1	不正利用事例と公式発表 セクションを 1 脆弱性が弊社販売代理店 要求の作業の間に検出されたことを示すために修正しました。			2010-September-23
1.0	Initial public release.			2010-September-22

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。