

# Cisco IOSおよびIOS XEソフトウェアのH.323メッセージ検証におけるDenial of Service(DoS)の脆弱性



アドバイザーID : cisco-sa-20160928-h323 [CVE-2016-6384](#)  
初公開日 : 2016-09-28 16:00  
バージョン 1.0 : Final  
CVSSスコア : [7.8](#)  
回避策 : No workarounds available  
Cisco バグ ID : [CSCux04257](#)

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およびIOS XEソフトウェアのH.323サブシステムの脆弱性により、認証されていないリモート攻撃者が該当デバイスでサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、H.323プロトコルスイートメッセージの特定のフィールドを適切に検証できないことに起因します。悪意のあるメッセージを処理する際に、該当デバイスが無効なメモリ領域にアクセスを試み、クラッシュが発生する可能性があります。脆弱性を引き起こすように設計されたH.323パケットを送信できる攻撃者は、該当するデバイスをクラッシュさせて再起動させ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。この脆弱性に対処する回避策はありません。

このアドバイザーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-h323>

このアドバイザーは、2016年9月28日に公開された11件の脆弱性に関する10件のシスコセキュリティアドバイザーを含むCisco IOSソフトウェアおよびIOS XEソフトウェアリリースのセキュリティアドバイザーバンドルの一部です。このすべての脆弱性はセキュリティへの影響が「高」と評価されています。アドバイザーとリンクの一覧については、『[Cisco Event Response: September 2016 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication](#)』を参照してください。

# 該当製品

## 脆弱性のある製品

この脆弱性は、H.323メッセージを処理するように設定され、該当するCisco IOSおよびIOS XEソフトウェアリリースを実行しているシスコデバイスに影響を与えます。Cisco IOSおよびIOS XEソフトウェアの最近のリリースでは、デフォルトでH.323メッセージが処理されません。

脆弱性が存在する Cisco IOS ソフトウェアおよび IOS XE ソフトウェアのリリースについては、このアドバイザリの「[修正済みソフトウェア](#)」の項を参照してください。

Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行しているデバイスがH.323メッセージを処理しているかどうかを確認するには、`show process cpu | include H323`コマンドを実行します。次に例を示します。

```
<#root>

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#
```

前記の例では、CCH323\_CTおよびCCH323\_DNSプロセスがデバイスで実行されています。したがって、デバイスはH.323メッセージをリスンしています。これらのプロセスまたは同様のH.323関連のプロセスのいずれかがアクティブな場合、デバイスは脆弱です。

注：Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行しているデバイスがH.323メッセージの処理を開始する方法は複数あるため、`show process cpu | include H323`コマンドを使用します。

## Cisco IOS ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS ソフトウェア リリースは、管理者がデバイスにログインして、コマンドライン インターフェイス (CLI) で `show version` コマンドを使用し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS ソフトウェアを実行している場合、システム バナーに「Cisco Internetwork Operating System Software」や「Cisco IOS Software」などのテキストが表示されます。バナーにはインストールされたイメージ名もカッコ内に表示され、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。一部のシスコ デバイスでは、`show version` コマンドをサポートしてい

なかったり、別の出力が表示されたりします。

次の例は、Cisco IOS ソフトウェア リリースが 15.5(2)T1 で、インストールされたイメージ名が C2951-UNIVERSALK9-M であるシスコ製品を示しています。

```
<#root>
```

```
Router>
```

```
show version
```

```
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
.
.
```

Cisco IOS ソフトウェアリリースの命名と番号付けの規則に関する詳細は、『[White Paper: Cisco IOS and NX-OS Software Reference Guide](#)』を参照してください。

## Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で show version コマンドを実行し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「Cisco IOS XE Software」などのテキストが表示されます。

次に、Cisco IOS XE ソフトウェア リリース 3.16.1aS が実行されているデバイスでの show version コマンドの出力例を示します。

```
<#root>
```

```
Router>
```

```
show version
```

```
Cisco IOS XE Software, Version 03.16.01a.S - Extended Support Release
Cisco IOS Software, ASR1000 Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(3)S1a, RELEASE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Nov-15 17:40 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェアリリースの命名と番号付けの規則に関する詳細は、『[White Paper:](#)

[Cisco IOS and NX-OS Software Reference Guide](#)』を参照してください。

## 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。

シスコは、この脆弱性が Cisco IOS XR ソフトウェアまたは Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

## 回避策

この脆弱性に対処する回避策はありません。

## 修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェアバージョンとフィーチャセットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

<http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN.html>

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンスアップグレードです。無償のセキュリティソフトウェアアップデートによって、お客様に新しいソフトウェアライセンス、追加ソフトウェアフィーチャセット、またはメジャーリビジョンアップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート ( Cisco Security Advisories and Alerts ) ] ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける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。

### サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、

Cisco Technical Assistance Center ( TAC ) に連絡してアップグレードを入手してください。

[http://www.cisco.com/c/ja\\_jp/support/web/tsd-cisco-worldwide-contacts.html](http://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html)

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

## Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、特定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース ( 「First Fixed」 ) を特定できます。また該当する場合、そのリリースに関するすべてのアドバイザリの脆弱性が修正された最初のリリース ( 「Combined First Fixed」 ) を特定できます。

このツールを使用して次のタスクを実行できます。

- ドロップダウン メニューからリリース ( 複数可 ) を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- show version コマンドの出力をツールで解析する
- カスタマイズした検索 ( 過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど ) を作成する

公開されたシスコ セキュリティ アドバイザリのいずれかに該当するリリースであるかどうかを確認するには、Cisco.com の [Cisco IOS ソフトウェアチェッカー](#) を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアのリリース番号 ( たとえば、15.1(4)M2、3.1.4S など ) を入力します。

 オン

Cisco IOS XEソフトウェアリリースとCisco IOSソフトウェアリリースのマッピングについては、Cisco IOS XEソフトウェアのリリースに応じて「[Cisco IOS XE 2 Release Notes](#)」、「[Cisco IOS XE 3S Release Notes](#)」、または「[Cisco IOS XE 3SG Release Notes](#)」を参照してください。

## 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。

## 出典

この脆弱性は、Cisco TACによるお客様のケースの調査中に発見されました。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-h323>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2016年9月28日

## 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、単独の転載や意識を施した場合、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。