

Cisco IOS および IOS XE ソフトウェア H.323 メッセージ検証 サービス拒否の脆弱性

High

アドバイザリー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はリモート攻撃者非認証が影響を受けたデバイスのサービス拒否 (DoS) 条件を作成するようにする可能性があります。

脆弱性はきちんと H.323 プロトコル 스위트 メッセージのある特定のフィールドを検証する失敗が原因です。悪意のあるメッセージを処理するとき、影響を受けたデバイスはクラッシュに終って無効なメモリ領域に、アクセスするように試みるかもしれません。脆弱性を誘発するように設計されている H.323 パケットを入れることができる攻撃者により影響を受けたデバイスはクラッシュし、再起動します可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

[928-h323](#)

このアドバイザリーは、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 アドバイザリーを含む 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 アドバイザリー 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。これらのアドバイザリーとリンクの一覧については、以下を参照してください。 [シスコのイベント対応 : Cisco IOS および IOS XE ソフトウェアに関するセキュリティ アドバイザリー公開資料 \(半年刊、2016 年 9 月\)](#)

該当製品

脆弱性のある製品

H.323 メッセージを処理するために設定される IOS XE ソフトウェア リリースおよびこの脆弱性は影響を受けた Cisco IOS を実行する Cisco デバイスに影響を与えます。Cisco IOS の最新のリリースおよび IOS XE ソフトウェアは H.323 メッセージをデフォルトで処理しません。

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 ソフトウェアが Cisco IOS XE ソフトウェアを実行するデバイスが H.323 メッセージを処理しているかどうかを判別するために、`show process CPU` を使用して下さい | 次の例に示すように 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#
```

前述の例では、CCH323_CT および CCH323_DNS プロセス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または同じような H.323 関連のプロセスのうちのどれかがアクティブである場合脆弱です。

注: H.323 メッセージを処理し始めるように Cisco IOS ソフトウェアが Cisco IOS XE ソフトウェアを実行するデバイスのための複数の方法があるので Cisco は `show process CPU` を使用することを推奨します | デバイスが H.323 メッセージを処理しているかどうかを判別する特定の設定コマンドの代わりに H323 コマンドを **含んで下さい**。

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ます。その後ろには Cisco IOS ソフトウェアのリリース番号とリリース名も表示されます。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することがあります。

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。

```
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ついては、以下を参照してください。 [ホワイトペーパー：Cisco IOS および NX-OS ソフトウェア リファレンス ガイド](#)

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。

```
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 SOFTWARE (fcl)
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ついては、以下を参照してください。 [ホワイトペーパー：Cisco IOS および NX-OS ソフトウェア リファレンス ガイド](#)

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 アップデートを提供しています。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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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、[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/en/US/support/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

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できるよう、シスコでは [Cisco IOS Software Checker](#) ツールを提供しています。このツールにより、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、すべてのアドバイザリに記載されたすべて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

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含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全アドバイザリを含めるなど) を作成する

リリースが、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かどうかを確認するには、Cisco.com の [Cisco IOS Software Checker](#) 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 リリース (たとえば、15.1(4)M2、3.1.4S など) を入力します。

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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) では、本アドバイザリに記載されている脆弱性のエクスプロイト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 によって顧客の例の調査の間に検出されました。

URL

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-h323>

改訂履歴

Version	Description	Section	Status	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。