

# Cisco IOSおよびCisco IOS XEソフトウェアのTCPにおけるDenial of Service(DoS)の脆弱性

<b>Medium</b>	アドバイザーID : cisco-sa-20160620-isr	<a href="#">CVE-2015-6289</a>
<b>m</b>	初公開日 : 2016-06-20 20:45	
	最終更新日 : 2016-10-19 14:36	
	バージョン 1.3 : Final	
	CVSSスコア : <a href="#">5.0</a>	
	回避策 : No workarounds available	
	Cisco バグ ID : <a href="#">CSCvb66994</a> <a href="#">CSCuu13476</a>	

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Cisco IOS XEソフトウェアにおけるリモートTCP接続の処理における脆弱性により、認証されていないリモートの攻撃者が、メモリ不足による部分的なサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、該当デバイスへのリモート接続で不正または無効なTCPパケットが処理されることに起因します。攻撃者は、デバイスに接続し、不正または無効なフラグを持つ巧妙に細工されたTCPパケットを送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は低メモリ警告をデバイスに報告させ、結果的に部分的なDoS状態を引き起こす可能性があります。この脆弱性は当初、セキュアシェルホスト(SSH)リモート接続で発見されましたが、デバイスへの他のリモート接続にも影響を与える可能性があります。

シスコでは、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する予定です。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-20160620-isr>

## 該当製品

### 脆弱性のある製品

Cisco IOSおよびCisco IOS XEソフトウェアには脆弱性が存在します。

## 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。

## 回避策

この脆弱性を軽減する回避策はありません。

## 修正済みソフトウェア

シスコでは、Cisco Bugsの修正済みソフトウェアに関する情報を提供しています。この情報には、[Cisco Bug Search Tool](#)からアクセスできます。

ソフトウェアのアップグレードを検討する場合は、<http://www.cisco.com/go/psirt> の [Cisco Security Advisories and Responses](#) アーカイブや後続のアドバイザリを参照して、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。

## 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。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160620-isr>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.3	Cisco Bug ID CSCvb66994 ( 登録ユーザ専用 ) が追加されました。概要のスタイル編集 ( 技術的な変更なし )	Cisco Bug IDリスト、まとめ	Final	2016年10月19日
1.2	脆弱性がより一般的であることが判明したため、要約	タイトルと概要	Final	2016

	はSSH参照を削除するように変更されました。		I	年 10月 3日
1.1	この脆弱性は、Cisco IOSおよびIOS XEソフトウェアに影響を与えます。シスコはこの脆弱性に対するソフトウェアアップデートをリリースする予定です。	タイトル、脆弱性が存在する製品、および概要	Fina I	2016 年8月 18日
1.0	初回公開リリース	-	Fina I	2016 年 6 月 20 日

## 利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。