

Cisco IOSソフトウェアよくある産業プロトコル 要求サービス拒否の脆弱性

High

アドバイザーID : cisco-sa-
20160928-cip

[CVE-
2016-
6391](#)

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 : [CSCur69036](#)

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ソフトウェアのよくある産業プロトコル (CIP) 機能の脆弱性はリモート攻撃者非認証がサービス拒否 (DoS) 状態を作成するようにする可能性があります。

脆弱性は影響を受けたデバイスにきちんと珍しくの、しかし有効処理する失敗が原因要求のセットです。攻撃者は設計されている CIP Message 要求を入れることによって影響を受けたデバイスに脆弱性を誘発するようにこの脆弱性を不正利用する可能性があります。エクスプロイトはスイッチの機能を取り戻すようにデバイスの再起動が要求するトラフィックを処理することを止めるために原因になる可能性があります。

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。

このアドバイザーは、次のリンクより確認できます。

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

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。これらのアドバイザ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ー公開資料 \(半年刊、2016年9月 \)](#)

該当製品

CIP 機能は入手しやすい on Cisco 産業イーサネット スイッチ製品産業オートメーション アプリケーションのために使用されてであり。このプロトコルは、以前は Control and Information Protocol と呼ばれていました。

脆弱性のある製品

この脆弱性は CIP メッセージを処理するために影響を受けたデバイスが設定されるときだけ該当する Cisco IOS ソフトウェア リリースを実行する Cisco デバイスに影響を与えます。CIP 機能は、デフォルトでは無効です。

Cisco IOS ソフトウェア リリースが脆弱である情報に関しては、この状況報告の [修正済みソフトウェアのセクション](#)を参照して下さい。

CIP 機能がイネーブルになっているかどうか判別するために、**show running-config** を使用して下さい | **CIP enable** コマンドを含み、出力を戻すことを確認して下さい。次の例はデバイス示したものです Cisco IOS ソフトウェアをイネーブルになっている CIP 処理と動作します:

```
router#show running-config | include cip enable
cip enable
```

この脆弱性は影響を受けたデバイスの UDP ポート 2222 または 44818 に向かう IPv4 パケットとだけ不正利用することができます。TCP パケット、該当デバイスを通過するパケット、または IPv6 パケットで、この脆弱性が利用されることはありません。

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](#)

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 XE ソフトウェア、Cisco IOS XR ソフトウェア、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 ソフトウェア

顧客が Cisco IOSソフトウェアの脆弱性への公開を判別するのに助けるために Cisco はツールを、特定の Cisco IOS ソフトウェア リリースおよび諮問それぞれに説明がある脆弱性を解決する以前のリリースに影響を与える Cisco Security Advisory を識別する [Cisco IOSソフトウェアチェッカー](#) 提供します、(「最初に」 固定される)。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

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の [Cisco IOSソフトウェアチェッカー](#) を使用するか、または一次のフィールドで... Cisco IOS ソフトウェア リリースを—たとえば、15.1(4)M2 入力して下さい:

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 パートナーによって Cisco に報告されました。

URL

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

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。