

Cisco IOS ソフトウェアの Common Industrial Protocol 要求における Denial of Service (DoS) の脆弱性

High	アドバイザーID : cisco-sa-20170927-cip	CVE-2017-12234
	初公開日 : 2017-09-27 16:00	12234
	バージョン 1.0 : Final	CVE-2017-12233
	CVSSスコア : 8.6	2017-12233
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvc43709	
	CSCuz95334	

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 Common Industrial Protocol (CIP) 機能の実装における脆弱性により、認証されていないリモート攻撃者が該当デバイスのリロードを引き起こし、その結果、サービス妨害 (DoS) 状態が発生する可能性があります。

この脆弱性は、該当デバイス宛てに巧妙に細工された CIP パケットの不適切な解析に起因します。攻撃者は、該当デバイスに処理されるよう巧妙に細工した CIP パケットを送信することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生する可能性があります。

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。これら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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-cip>

このアドバイザーは、2017 年 9 月 27 日に公開された 13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリを含む 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 バンドルの一部です。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：9月2017年半年ごと Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書。](#)

該当製品

CIP 機能はシスコ産業用イーサネット スイッチ製品で共通して利用でき、産業用オートメーションアプリケーションで使用されます。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、Cisco IOS ソフトウェアの脆弱性が存在するリリースを実行し、かつ CIP 機能を有効にしているシスコ デバイスに影響を及ぼします。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、このアドバイザリの[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 機能が有効になるかどうか判別するために、管理者は `show running-config` を使用できます | `CIP enable` コマンドを CLI に含め、コマンドが出力を戻すことを確認して下さい。Cisco IOS Software が実行され、CIP 処理が有効になっている場合は、デバイスのコマンド出力が次のようになります。

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

```
  cip enable
```

この脆弱性の不正利用が可能なのは、該当デバイスの UDP ポート 2222 または 44818 宛ての IPv4 パケットの場合のみです。TCP パケット、該当デバイスを通るパケット、または IPv6 パケットで、この脆弱性が不正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、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 15.5(2)T1 を実行して、*C2951-UNIVERSALK9-M* のインストール済みイメージ名前があるデバイスのためのコマンドの出力を示したものです：

```
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、および 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。

セキュリティ侵害の痕跡

この脆弱性が不正利用されると、該当するデバイスがリロードされ、core ファイルが生成されます。core ファイルを検査し、脆弱性のエクスプロイトによるセキュリティ侵害が発生していないか確認するには、Cisco Technical Assistance Center (TAC) にご連絡ください。

回避策

これら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。

<https://www.cisco.com/c/en/us/products/end-user-license-agreement.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 TAC に連絡してアップグレードを入手してください。

<https://www.cisco.com/c/en/us/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 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、各アドバイザリに説明がある脆弱性を解決する以前のリリースおよび特定の Cisco IOS ソフトウェア 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」) を特定できません。

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

る脆弱性の不正利用事例とその公表は確認しておりません。

出典

この脆弱性は、シスコ内部でのシステム セキュリティ テストによって発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-cip>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 9 月 27 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。