Cisco IOS ソフトウェアの Common Industrial Protocol における複数の脆弱性

High

アドバイザリーID : cisco-sa-20150325-cip
初公開日 : 2015-03-25 16:00
最終更新日 : 2016-01-14 17:20
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCun49658 CSCun63514 CSCum98371

CVE-2015-0648
CVE-2015-0649
CVE-2015-0647

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）機能の実装には、巧妙に細工された CIP パケットを処理する際に以下の脆弱性があり、認証されていないリモート攻撃者がサービス妨害（DoS）状態を引き起こす可能性があります。

- Cisco IOS ソフトウェアの UDP CIP のサービス妨害（DoS）脆弱性
- Cisco IOS ソフトウェアの TCP CIP パケット メモリ リークに関する脆弱性
- Cisco IOS ソフトウェアの TCP CIP のサービス妨害（DoS）脆弱性

これらの脆弱性は、互いに独立して存在します。 いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

これらの脆弱性の不正利用が成功すると、認証されていないリモート攻撃者がフォワーディング プレーンのリロードを引き起こし、その結果、該当デバイスにサービスの中断が生じる可能性があります。 この脆弱性が繰り返し悪用されると、DoS 状態が続く可能性があります。

さらに、Cisco IOS ソフトウェアの TCP CIP パケット メモリ リークに関する脆弱性の不正利用が成功すると、認証されていないリモート攻撃者が該当デバイスにメモリ リークを引き起こす可能性があります。

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。 このアドバイザリは、次のリンクより確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-cip

注: 2015 年 3 月 25 日、Cisco IOS ソフトウェアおよび IOS XE ソフトウェアのセキュリティ アドバイザリにおいて、7 つの Cisco Security Advisory を含むバンドル資料を公開しました。 これらのアドバイザリは Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの脆弱性を扱っています。 個々の公表資料へのリンクは、次のリンクにある「*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 アドバイザリ公開資料*」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html

該当製品

脆弱性のある製品

Cisco IOS ソフトウェアの UDP CIP のサービス妨害（DoS）脆弱性

Cisco IOS ソフトウェアには、該当デバイスで CIP が設定されている場合に、UDP 経由の巧妙に細工された CIP パケットが処理されると、該当デバイスがリロードされる可能性のある脆弱性が存在します。

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 宛の IPv4 パケットのみです。 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。

認証されていないリモート攻撃者は、CIP が設定された該当デバイスの UDP ポート 2222 または 44818 に多くの巧妙に細工した IPv4 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。

トラフィック処理を行うインターフェイスで CIP が有効化されている場合、Cisco IOS ソフトウェアが影響を受ける可能性があります。 Cisco IOS ソフトウェアではデフォルトで、CIP は有効化されていません。

インターフェイスで CIP が有効になっているかどうかを確認するには、 **show running-config | include cip** 特権 EXEC コマンドを使用します。 「 **cip enable**」という文字列が **show running-config | include cip** の出力に現れた場合、CIP が有効化されています。

以下に、 **show running-config | include cip** コマンドを、CIP 機能を有効にした Cisco IOS ソフトウェアを実行しているデバイスで実行した場合の出力例を示します。

```
Switch# show running-config | include cip
 cip security password <output omitted>
 cip enable
```

Cisco IOS ソフトウェアの TCP CIP パケット メモリ リークに関する脆弱性

Cisco IOS ソフトウェアには、該当デバイスで CIP が設定されている場合に、TCP 経由の巧妙に細工された CIP パケットが処理されると、該当デバイスのメモリ リークが引き起こされ、最終的にリロードが発生する可能性のある脆弱性が存在します。

この脆弱性の不正利用が可能なのは、該当デバイスの TCP ポート 44818 宛の IPv4 パケットのみです。 UDP 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、この脆弱性が不正利用されることはありません。

認証されていないリモート攻撃者は、CIP が設定された該当デバイスの TCP ポート 44818 に多数の巧妙に細工した IPv4 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。

この脆弱性を不正利用するには、TCP スリーウェイ ハンドシェイクが正常に確立されていることが必要です。

トラフィック処理を行うインターフェイスで CIP が有効化されている場合、Cisco IOS ソフトウェアが影響を受ける可能性があります。 Cisco IOS ソフトウェアではデフォルトで、CIP は有効化されていません。

インターフェイスで CIP が有効になっているかどうかを確認するには、 **show running-config | include cip** 特権 EXEC コマンドを使用します。 「 **cip enable**」という文字列が **show running-config | include cip** コマンドの出力に現れた場合、CIP が有効化されています。

以下に、 **show running-config | include cip** コマンドを、CIP 機能を有効にした Cisco IOS ソフトウェアを実行しているデバイスで実行した場合の出力例を示します。

```
Switch# show running-config | include cip
 cip security password <output omitted>
 cip enable
```

Cisco IOS ソフトウェアの TCP CIP のサービス妨害（DoS）脆弱性

Cisco IOS ソフトウェアには、該当デバイスで CIP が設定されている場合に、TCP 経由の巧妙に細工された CIP パケットが処理されると、該当デバイスがリロードされる可能性がある脆弱性が存在します。

この脆弱性の不正利用が可能なのは、該当デバイスの TCP ポート 44818 宛の IPv4 パケットのみです。 UDP 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、この脆弱性が不正利用されることはありません。

認証されていないリモート攻撃者は、CIP が設定された該当デバイスの TCP ポート 44818 に多数の巧妙に細工した IPv4 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。

この脆弱性を不正利用するには、TCP スリーウェイ ハンドシェイクが正常に確立されていることが必要です。

トラフィック処理を行うインターフェイスで CIP が有効化されている場合、アクセス ポイントの Cisco IOS ソフトウェアが影響を受ける可能性があります。 Cisco IOS ソフトウェアではデフォルトで、CIP は有効化されていません。

インターフェイスで CIP が有効になっているかどうかを確認するには、 **show running-config | include cip** 特権 EXEC コマンドを使用します。 「 **cip enable**」という文字列が **show running-config | include cip** コマンドの出力に現れた場合、CIP が有効化されています。

以下に、 **show running-config | include cip** コマンドを、CIP 機能を有効にした Cisco IOS ソフトウェアを実行しているデバイスで実行した場合の出力例を示します。

```
Switch# show running-config | include cip
 cip security password <output omitted>
 cip enable
```

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 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た場合は、デバイスが Cisco IOS ソフトウェアを実行しています。 カッコ内にイメージ名が表示され、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続きます。 他のシスコ デバイスでは、**show version** コマンドが存在しなかったり、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 15.2(4)M5、インストールされたイメージ名が C3900-UNIVERSALK9-M であるシスコ製品を示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

Cisco IOS ソフトウェア リリースの命名規則については、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

Cisco IOS XR ソフトウェアは、これらの脆弱性の影響を受けません。

Cisco IOS XE ソフトウェアは、これらの脆弱性の影響を受けません。

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。

詳細

Common Industrial Protocol（CIP）は、産業オートメーション アプリケーション用の産業プロトコルです。 このプロトコルは、DeviceNet、EtherNet/IP、CIP Safety および CIP sync などの CIP に基づいたネットワーク テクノロジーをサポートする組織である、Open DeviceNet Vendors Association（ODVA）によってサポートされています。 CIP では、明示的メッセージングには UDP/TCP ポート 44818、暗黙的メッセージングには UDP ポート 2222 を使用します。

Cisco IOS ソフトウェアの UDP CIP のサービス妨害（DoS）脆弱性

Cisco IOS ソフトウェアの Common Industrial Protocol（CIP）機能の脆弱性により、認証されていないリモート攻撃者が該当デバイスのリロードを引き起こす可能性があります。

この脆弱性は、CIP ポート宛の不正な UDP パケットの不適切な処理に起因します。 攻撃者は、該当デバイスで CIP が有効にされている場合に、CIP ポート宛の不正な UDP 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、攻撃者は該当デバイスのリロードを引き起こす可能性があります。

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 宛の IPv4 パケットのみです。 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。

本脆弱性は、Cisco Bug ID CSCum98371（ 登録ユーザ専用 ）として文書化されており、Common Vulnerabilities and Exposures（CVE）ID CVE-2015-0647 が割り当てられています。

Cisco IOS ソフトウェアの TCP CIP パケット メモリ リークに関する脆弱性

Cisco IOS ソフトウェアの Common Industrial Protocol（CIP）機能の脆弱性により、認証されていないリモート攻撃者が該当デバイスのメモリ リークを引き起こす可能性があります。

この脆弱性は、CIP ポート宛の TCP パケット シーケンスの不適切な処理に起因します。 攻撃者は、該当デバイスで CIP が有効にされている場合に、CIP ポート宛に細工したシーケンスの 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、攻撃者は該当デバイスのリロードを引き起こす可能性があります。

この脆弱性の不正利用が可能なのは、該当デバイスの TCP ポート 44818 宛の IPv4 パケットのみです。 UDP 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。

本脆弱性は、Cisco Bug ID CSCun49658（ 登録ユーザ専用 ）として文書化され、CVE ID CVE-2015-0648 が割り当てられています。

Cisco IOS ソフトウェアの TCP CIP のサービス妨害（DoS）脆弱性

Cisco IOS ソフトウェアの Common Industrial Protocol（CIP）機能の脆弱性により、認証されていないリモート攻撃者が該当デバイスのリロードを引き起こす可能性があります。

この脆弱性は、CIP ポート宛の不正な TCP パケットの不適切な処理に起因します。 攻撃者は、該当デバイスで CIP が有効にされている場合に CIP ポート宛に不正な 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、攻撃者は該当デバイスのリロードを引き起こす可能性があります。

この脆弱性の不正利用が可能なのは、該当デバイスの TCP ポート 44818 宛の IPv4 パケットのみです。 UDP 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。

本脆弱性は、Cisco Bug ID CSCun63514（ 登録ユーザ専用 ）として文書化され、CVE ID CVE-2015-0649 が割り当てられています。

回避策

これらの脆弱性を軽減する回避策はありません。

ネットワーク内のシスコ デバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Mitigation Bulletin』を参照してください。以下のリンクから入手できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=37513

修正済みソフトウェア

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, Responses, and Alerts アーカイブや、後続のアドバイザリを参照して侵害の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。

Cisco IOS ソフトウェア

シスコでは、Cisco IOS ソフトウェアの脆弱性にさらされているかどうかを判断するためのツールを提供しています。 Cisco IOS Software Checker により、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を選択するか、ローカル システムからファイルをアップロードすることによって、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、特定の資料のみ、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

このツールを使うことで、そのソフトウェア リリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（"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。 Cisco IOS Software Checker を参照するか、次のフィールドに Cisco IOS ソフトウェア リリースを入力して、いずれかの公開された Cisco IOS ソフトウェア アドバイザリに該当するかどうかを判断できます。

（入力例： 15.1(4)M2）

Cisco IOS ソフトウェア リリースへの Cisco IOS XE ソフトウェア リリースのマッピングについては、「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、および「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不正利用事例とその公表は確認しておりません。

本資料のすべての脆弱性は内部調査中に発見されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-cip

改訂履歴

Version	Description	Section	Status	日付
1.1	過去に公開されたすべてのCisco IOSソフトウェア セキュリティ アドバイザリを照会できる Cisco IOS Checker ソフトウェアの Checker フォームを更新しました。			2016 年 1 月 14 日
1.0	初回公開リリース			2015 年 3 月 25 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、単独の転載や意訳を施した場合、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。