シスコ産業用イーサネット スイッチの Cisco IOS ソフトウェアにおける PROFINET の Denial of Service の脆弱性

High

アドバイザリーID : cisco-sa-20170927-profinet

初公開日 : 2017-09-27 16:00

最終更新日 : 2017-09-28 11:23

バージョン 1.1 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCuz47179

CVE-2017-12235

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 PROFINET 検出および構成プロトコル（PN-DCP）の実装には脆弱性があり、認証されていないリモートの攻撃者が該当するデバイスのリロードを引き起こし、その結果、Denial of Service（DoS）の状態を発生させる可能性があります。

この脆弱性は、該当するデバイスに送信される PN-DCP のアイデンティティ要求入力の解析が不適切であることに起因します。 攻撃者が、該当するデバイスに巧妙に細工された PN-DCP のアイデンティティ要求パケットを送信し、その後に通常の PN-DCP のアイデンティティ要求パケットを送信し続けることで、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。

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-profinet

このアドバイザリは、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リ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

脆弱性のある製品

この脆弱性は、CiscoIOS ソフトウェアの脆弱なリリースを実行し、PROFINET のメッセージを処理するよう設定されたシスコ デバイスに影響を与えます。 Cisco IOS ソフトウェア リリース 12.2(52)SE 以降、PROFINET はすべてのベース スイッチ モジュールおよび拡張ユニットのイーサネット ポート上で、デフォルトで有効となっています。

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。

PROFINET 機能が無効であ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 **| profinet** 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。 次の例では、デバイスで Cisco IOS ソフトウェアが実行されており、PROFINET のメッセージを処理するように設定されていない場合の出力を示しています。この場合は、デバイスは脆弱ではありません。

```
router# show running-config | include profinet
no profinet
```

さらに PROFINET が有効に なったかどうか確認する、管理者は CLI で提示 **profinet status コマンドを**使用できます。 **profinet は**ハードウェアプラットフォームに **ステータス**ないことを Profinet のステータスが **無効**であるかまたはコマンドが **示せば**、デバイスは脆弱考慮されます。 次の例では、PROFINET のプロトコルが有効になっています。

```
router# show profinet status
Profinet : Enabled
```

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、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。

詳細

PROFINET は PROFIBUS International（PI）のオープンな産業用イーサネット標準であり、オートメーション コントロール用に TCP/IP および IT 標準を使用しています。 PROFINET は、装置およびテスト機器の動きや精度の制御が重要である工業オートメーション システムやプロセス制御ネットワークに特に有用です。 PROFINET はデータ交換を重視しており、速度要件に合った通信パスを定義しています。

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し、コア ファイルが生成されます。 このコア ファイルを確認し、デバイスにこの脆弱性の不正利用が発生していないかを判別するには、Cisco Technical Assistance Center（TAC）までご連絡ください。

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。
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ます。 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を助けるために 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—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

本脆弱性は、シスコ内部でのセキュリティ 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-profinet

改訂履歴

Version	Description	Section	Status	日付
1.1	管理者が Profinet が有効かどうかを判別する際に役立つ情報を追加しました。	脆弱性のある製品	Final	2017 年 9 月 28 日
1.0	初回公開リリース		Final	2017 年 9 月 27 日

利用規約