Cisco Prime Infrastructure の任意のファイル アップロードとコマンド実行における脆弱性

Critical

アドバイザリーID : cisco-sa-20181003-pi-tftp

初公開日 : 2018-10-03 16:00

バージョン 1.0 : Final

CVSSスコア : 7.3

回避策 : Yes

Cisco バグ ID : CSCvk24890

CVE-2018-15379

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 Prime Infrastructure (PI) の HTTP Web サーバに無制限のディレクトリ権限があるという脆弱性により、認証されていないリモートの攻撃者が任意のファイルをアップロードする可能性があります。 攻撃者はこのファイルを使用して、ユーザ prime の特権レベルでコマンドを実行する可能性があります。 このユーザには、管理者特権や root 特権はありません。

この脆弱性は、重要なシステム ディレクトリに対する誤ったアクセス許可の設定が原因で発生します。 攻撃者は、Web インターフェイスの GUI を使用してアクセス可能な TFTP を使用して悪意のあるファイルをアップロードすることで、この脆弱性をエクスプロイトできます。 エクスプロイトに成功した攻撃者は、認証されていないターゲットのアプリケーションでコマンドを実行する可能性があります。

シスコ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しました。 本脆弱性に対処する回避策がいくつかあります。

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-20181003-pi-tftp

該当製品

脆弱性のある製品

TFTP サーバが有効 (デフォルトの設定) になっている場合、最初の修正済みリリースより前の Cisco PI ソフトウェア リリース 3.2 ~ 3.4 には脆弱性があります。 管理者は、Web インタ

ーフェイスで [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [サーバ（Server）] > [TFTP] を選択して、TFTP のステータスを確認できます。

PI 連邦情報処理標準（FIPS）イメージでは、TFTP はデフォルトで無効になっています。

PI ソフトウェア リリースの確認

アプライアンスで実行されているソフトウェア リリースを確認するために、次のいずれかの方法を使用できます。

- 管理者はコンソール CLI で **show version** コマンドを発行できます。 以下に、PI メンテナンス リリース 3.2.2 をインストールした PI ソフトウェア リリース 3.2.0 を実行している影響を受けるアプリケーションからの出力を示します。

```
piconsole# show version
Cisco Application Deployment Engine OS Release: 3.2
ADE-OS Build Version: 3.2.0.001
ADE-OS System Architecture: x86_64

Copyright (c) 2009-2016 by Cisco Systems, Inc.
All rights reserved.
Hostname: lmpy-spc-princess

Version information of installed applications
---------------------------------------------

Cisco Prime Infrastructure
**********************************************************
Version : 3.2.0
Build : 3.2.0.0.132
Critical Fixes:
PI 3.2.2 Maintenance Release ( 6.0.0 )
Device Support:
Prime Infrastructure 3.2 Device Pack 11 ( 11.0 )
```

- また、管理者は **http(s): //<system-ip>** URL Web PI PI ソフトウェア リリースはウェルカム画面に表示されます。管理者は [インストール済みの更新プログラムの表示（View Installed Update）] をクリックして PI メンテナンス リリースおよびパッチの一覧を含むポップアップ ウィンドウを開くことができます。 以下に、PI ソフトウェア リリース 3.2 でポップアップ ウィンドウに表示されるテキストの表示例を示します。

```
Cisco Prime Infrastructure
Version 3.2
View Installed Update
```

ポップアップ ウィンドウには次の形式でメンテナンス リリース更新プログラムが一覧表示されます。

```
Update Name
PI 3.2.2 Maintenance Release
```

- また、管理者は **http(s): //<system-ip>** URL Web 、[歯車（Gear）] > [Prime Infrastructure （About Prime Infrastructure）] > [表示（View Installed Updates）] 画面PI リリース情報は次のように表示されます。

```
Installed Updates

Critical Fixes
Update Name Version
PI 3.2.2 Maintenance Rel...    6.0.0
```

```
Device Support
Update Name
Prime Infrastructure 3.2
```

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

シスコでは、Cisco Evolved Programmable Network Manager（EPNM）には脆弱性が存在しないことを確認しています。

回避策

管理者は、Web インターフェイスで [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [サーバ（Server）] > [TFTP] を選択して、Cisco PI の TFTP を無効化できます。 Cisco PI では、TFTP は、イメージ転送、設定、アーカイブなどの内部操作に使用されます。 管理者は、代わりに Secure Copy Protocol（SCP）や SFTP などのセキュアなプロトコルをこれらの機能に使用することができます。

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は新規リリースでも継続して適切なサポートが受けられることを確

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。

修正済みリリース

次の表に示すように、適切なリリースにアップグレードする必要があります。

Cisco Prime Infrastructure メジャー リリース	この脆弱性に対する最初の修正リリース
3.2	3.3.1 Update 02
3.2 FIPS	修正プログラムはありません[1]
3.3	3.3.1 Update 02
3.4	3.4.1

1. TFTP は Cisco PI リリース 3.2 FIPS ではデフォルトで無効になっています。 管理者は、このアドバイザリで提供されている回避策を使用することもできます。

ソフトウェアのダウンロード

Cisco Prime Infrastructure ソフトウェアは、Cisco.com の Software Center から次の手順でダウンロードできます。

- [すべて参照（Browse all）] をクリックします。
- [クラウドおよびシステム管理（Cloud and Systems Management）] > [ルーティングおよびスイッチングの管理（Routing and Switching Management）] > [ネットワーク管理ソリューション（Network Management Solutions）] > [Prime Infrastructure] を選択します。
- ソフトウェア ダウンロード ナビゲーションの右側のペインを使用して、Cisco PI のリリースにアクセスします。

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

シスコは、Beyond Security's SecuriTeam Secure Disclosure プログラムにこの脆弱性をご報告いただいた個人のセキュリティ研究者である Pedro Ribeiro 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-pi-tftp

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2018 年 10 月 3 日

利用規約