Cisco IOS および IOS XE ソフトウェア スマートなインストール サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20160323-smi
初公開日 : 2016-03-23 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 : CSCuv45410

CVE-2016-1349

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 および IOS XE ソフトウェアのスマートなインストール クライアント機能により非認証を可能にする可能性がある影響を受けたデバイスのサービス拒否（DoS）条件を引き起こすために脆弱性がリモート攻撃者含まれています。

脆弱性はイメージリスト パラメータの不正確な処理が原因です。 攻撃者は TCPポート 4786 へ巧妙に細工されたスマートなインストール パケットを送信 することによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトにより Cisco Catalyst スイッチは DoS 状態に終って、リロードします可能性があります。

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。脆弱なデバイスのスマートなインストール機能をディセーブルにすること以外この脆弱性に対処する回避策がありません。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-smi

この状況報告は、6 脆弱性を記述する 6 Cisco Security Advisory を含む 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のリリースの 2016 年 3月 23 日一部です。 すべての脆弱性にあります「最高のセキュリティ への影響定格が」。 それらへの状況報告およびリンクの完全なリストに関しては、 Cisco イベント応答が表示されて下さい : 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

Cisco IOS および IOS XE ソフトウェアのスマートなインストール クライアント機能は新しいスイッチにゼロ タッチ配備を提供するプラグアンドプレイ設定およびイメージ管理機能です。 機能は顧客が Ciscoスイッチをあらゆる位置に出荷し、ネットワークにインストールし、追加コンフィギュレーション必要条件なしで動力を与えることを可能にします。

脆弱性のある製品

この脆弱性はスマートなインストール クライアント機能がイネーブルの状態で Cisco IOS または IOS XE ソフトウェアの脆弱なリリースを実行している Ciscoデバイスに影響を与えます。 Cisco IOS および IOS XE 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」セクションを参照して下さい。

Cisco IOS か IOS XE デバイスがスマートなインストール クライアント機能がイネーブルの状態で設定されるかどうか判別するためにスマートなインストール クライアントの **提示 vstack config** privileged exec コマンドを使用して下さい。 以下はスマートなインストール クライアントで設定される Cisco Catalyst スイッチの **提示 vstack config コマンド**の出力です。 **ロール**のための出力 : **提示 vstack config コマンド**からの **クライアントは**機能がデバイスでイネーブルになっていることを確認します。

```
switch#show vstack config
 Role: Client  Vstack Director IP address: 10.1.1.100
```

注: スマートなインストール クライアントの機能性はイネーブルになられていたデフォルトで on Cisco IOS スイッチです。

注: スマートなインストール ディレクターで設定される Ciscoデバイスはこの脆弱性から影響を受けません。

注: リリースが稼働しているスイッチは Cisco IOS ソフトウェア リリース 12.2(52)SE より先に可能なスマートではないインストールではないです **archive download-sw** privileged exec コマンドをサポートする場合スマートなインストール クライアントである場合もあります。

Cisco IOS または IOS XE ソフトウェア リリースの判別

、管理者はデバイスにログインどの Cisco IOS ソフトウェア リリースが Cisco製品で動作しているか判別し、**show version コマンドを**コマンドラインインターフェイスで使用し、次に現われるシステムバナーを参照するためにできます。 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。 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 XR ソフトウェアまたは 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

この脆弱性の不正利用により影響を受けたデバイスは *crashinfo ファイル*をリロードし、生成します。 ファイルを検討し、デバイスがこの脆弱性の不正利用によって妥協されたかどうか判別するために Cisco Technical Assistance Center （ TAC ）に連絡して下さい。

回避策

利用可能なスマートなインストール機能をディセーブルにすること以外この脆弱性に対処する回避策がありません。 スマートなインストール機能はクライアントでデフォルトで切り替えますイネーブルになっています。 設定はクライアントで切り替えます必要とされません。

Cisco IOS および IOS XE ソフトウェアのある特定のリリースでは、スマートなインストール クライアント機能はグローバル 設定 コマンドで **vstack** ディセーブルにすることができません。 Cisco IOS およびコマンドが利用できる IOS XE ソフトウェアのある特定のリリースでは、脆弱性はスマートなインストール クライアント機能をディセーブルにすることによって対処することができます。

次の例はスマートなインストール クライアント機能がディセーブルの状態で Cisco Catalyst スイッチで **提示 vstack config コマンド**の出力を示したものです:

```
switch#show vstack config
 Role: Client (SmartInstall disabled)
```

```
Vstack Director IP address: 10.1.1.100
```

注: スマートなインストール クライアント機能を無効に する **vstack** グローバル 設定 コマンドは Ciscoバグ CSCtj75729 （ *TCPポートのスマートなインストール デフォルトサービスをのための修正で 4786) 締める能力*もたらされませんでした。 Cisco IOS か IOS XE ソフトウェアのリリースサポートがスマートなインストール クライアント機能しかし **vstack** コマンドない場合、リリースは Ciscoバグ CSCtj75729 のための修正が含まれていません。

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場合は、http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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 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 および IOS XE ソフトウェア

顧客が Cisco IOS および IOS XE 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、特定のソフトウェア 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）。 該当する場合、ツールはまた識別されるすべての状況報告に説明があるすべての脆弱性を解決する以前のリリースを戻します（「結合される最初に」固定される）。

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 か IOS XE ソフトウェア リリースを—たとえば、**15.1(4)M2** か **3.01.4S** 入力して下さい:

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「 Cisco IOS XE 2 Release Notes」、「 Cisco IOS XE 3S Release Notes」、または「 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

この脆弱性は維持可能なネットワーク セキュリティによって Cisco に発見され、報告されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-smi

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2016-March-23

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。