Cisco IOS および IOS XE ソフトウェア スマートなインストール メモリリークの脆弱性

High

アドバイザリーID : cisco-sa-20160928-smi

初公開日 : 2016-09-28 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 : CSCuy82367

CVE-2016-6385

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メモリリークおよび終局サービス拒否（DoS）状態を引き起こすために脆弱性リモート攻撃者が含まれています。

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 スイッチはメモリをリークさせ、結局 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。影響を受けた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-20160928-smi

このアドバイザリは、2016 年 9 月 28 日に公開された 11 件の脆弱性に関する 10 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。 このすべての脆弱性はセキュリティへの影響が「高」と評価されています。 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： 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（半年刊、2016 年 9 月）

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ソフトウェアまたは Cisco 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。

脆弱性が存在する Cisco IOS ソフトウェアおよび IOS XE ソフトウェアのリリースについては、このアドバイザリの「 修正済みソフトウェア」の項を参照してください。

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。 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。 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。

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
```

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、コマンドライン インターフェイス (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]

Cisco IOS XE 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 XE 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**を実行し、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 XE ソフトウェアを実行している場合、システム バナーに「*Cisco IOS XE Software*」などのテキストが表示されます。

次に、Cisco IOS XE ソフトウェア リリース 3.16.1aS が実行されているデバイスでの **show version** コマンドの出力例を示します。

```
Router> show version
Cisco IOS XE Software, Version 03.16.01a.S - Extended Support Release
Cisco IOS Software, ASR1000 Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(3)S1a,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Nov-15 17:40 by mcpre
.
.
.
```

Cisco IOS XE 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メモリをリークさせ、結局リロードします

。

回避策

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: 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*をのための修正と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 コマンドの使用は *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 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

Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるよう、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、特定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「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、公開されたシスコ セキュリティ アドバイザリのいずれかに該当するかどうかを確認するには、Cisco.com の Cisco IOS Software Checker を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェア リリース（たとえば、**15.1(4)M2**、**3.1.4S** など）を入力します。

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

この脆弱性はサポート ケースの解決中に発見されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-smi

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2016 年 9 月 28 日

利用規約