Cisco IOS および IOS XE ソフトウェアの Smart Install 機能における Denial of Service（DoS）の脆弱性

アドバイザリーID : cisco-sa-20180328-smi
初公開日 : 2018-03-28 16:00
最終更新日 : 2022-12-15 22:19
バージョン 1.7 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvd40673
CVE-2018-0156

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 ソフトウェアと Cisco IOS XE ソフトウェアの Smart Install 機能における脆弱性により、認証されていないリモート攻撃者が影響を受けるデバイスのリロードを引き起こし、その結果サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、パケット データの不適切な検証に起因します。攻撃者は、該当デバイスの TCP ポート 4786 番宛に巧妙に細工されたパケットを送信することにより、この脆弱性を不正利用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ています。この脆弱性に対処する回避策はありません。

Smart Installクライアント機能は、Cisco Bug ID CSCvd36820に対処するアップデートが実施されていないソフトウェアリリースが稼働するスイッチでは、デフォルトで有効になっています。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi

このアドバイザリは、2018年3月28日に公開された22件の脆弱性に関する20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。アドバイザリとリンクの一覧については、『Cisco Event Response: March 2018 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、Smart Install クライアント機能が有効化され、脆弱性が存在する Cisco IOS ソフトウェア リリースまたは IOS XE ソフトウェア リリースを実行するシスコ デバイスに影響を与えます。

Smart Install クライアントのスイッチのみが、本アドバイザリで説明されている脆弱性の影響を受けます。Smart Install ディレクタとして設定されているシスコ デバイスはこの脆弱性の影響を受けません。

Smart Install をサポートするデバイスの一覧については、『Cisco Smart Install コンフィギュレーション ガイド』の「Smart Install でサポートされるデバイス」の項を参照してください。

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。

特定のリリースに関する注意事項

Smart Installクライアント機能は、Cisco Bug ID CSCvd36820に対処するアップデートが実施されていないソフトウェアリリースが稼働するスイッチでは、デフォルトで有効になっています。

Cisco IOS ソフトウェア リリース 12.2(52)SE よりも前のリリースを実行するスイッチは Smart Install 対応ではありませんが、archive download-sw 特権 EXEC コマンドをサポートしている場合、Smart Install クライアントにすることができます。

Smart Install クライアント機能が有効かどうかの判断

デバイスで Smart Install クライアント機能が有効化されているかどうかを確認するには、Smart Install クライアントで show vstack config 特権 EXEC コマンドを使用します。show vstack configコマンドのRole: Client（クライアント）およびOper Mode: EnabledまたはRole: Client（SmartInstall有効）の出力で、デバイスで機能が有効になっていることを確認します。

次の例は、Smart Install クライアントとして設定された Cisco Catalyst スイッチでの show vstack config コマンドの出力結果を示します。

```
<#root>

switch1#

show vstack config
```

```
Role: Client (SmartInstall enabled)


 .
 .
 .

switch2#

show vstack config


 Capability: Client

Oper Mode: Enabled



Role: Client


 .
 .
 .
```

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、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します。

次に、Cisco IOS ソフトウェア リリース 15.5(2)T1 が実行されていて、インストールされているイメージ名が C2951-UNIVERSALK9-M であるデバイスでのコマンド出力例を示します。

```
<#root>

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関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

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 Software」、「Cisco IOS XE Software」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 が実行されていて、インストールされているイメージ名が CAT3K_CAA-UNIVERSALK9-M であるデバイスでのコマンドの出力例を示します。

<#root>

```
ios-xe-device#
```

```
show version
```

```
Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali 16.2.1, REL
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 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関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

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。

詳細

Cisco Smart Install とは、新しい（通常はアクセス レイヤ）スイッチのゼロタッチ導入を実現するための「プラグアンドプレイ」構成およびイメージ管理機能です。この機能により、お客様は、スイッチを追加設定することなく出荷し、ネットワークに設置して電源を投入するだけで使い

始めることができます。Smart Install 機能は、仕様上認証を備えていません。

Smart Install ネットワークは、1 台の Smart Install ディレクタ スイッチまたはルータ（統合ブランチ ディレクタ（IBD）とも呼ばれる）、1 台以上の Smart Install クライアント スイッチ（統合ブランチ クライアント（IBC）とも呼ばれる）で構成されます。クライアント・スイッチをダイレクタに直接接続する必要はありません。クライアント・スイッチは最大7ホップ離れた場所に配置できます。

ディレクタは、クライアント スイッチのイメージおよびコンフィギュレーションの単一管理ポイントとなります。クライアント スイッチが最初にネットワークに設置されると、ディレクタがその新しいスイッチを自動的に検出し、ダウンロードする適正な Cisco IOS ソフトウェア イメージとコンフィギュレーション ファイルを特定します。また、ディレクタはクライアントに IP アドレスとホスト名を割り当てることができます。

回避策

Cisco Smart Install を使用する必要がある場合、本脆弱性の回避策はありません。必要ない場合は、no vstack コマンドで Cisco Smart Install 機能を無効にすることができます。Cisco Bug ID CSCvd36820に関連するソフトウェアリリースでCisco Smart Installを使用しない場合、この機能は自動的に無効になります。

Cisco Smart Install プロトコルの誤用に関するセキュリティ アドバイザリの情報と『Cisco Smart Install コンフィギュレーション ガイド』を参照することをお勧めします。

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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、[シスコのセキュリティアドバイザリおよびアラート（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 Cisco Service Contract 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 POS 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 および IOS XE ソフトウェア

お客様が 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するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、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、そのリリースに関する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。

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 リストからリリース（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入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべての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、3.13.8Sなど)を入力します。

	オン

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）は、2022 年 3 月に、この脆弱性のさらなるエクスプロイトが試みられたことを認識しました。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.7	エクスプロイトに関する情報を更新。	不正利用事例と公式発表	Final	2022年12月15日
1.6	メタデータを更新。Cisco Catalyst 6500 および 6800 シリーズ スイッチは脆弱ではないことが確認されたため、脆弱性のあるリリースが少なくなることが判明。修正に伴って IOS ソフトウェア チェッカーを更新。	—	Final	2018年5月3日
1.5	IOS Software Checker にて、脆弱であることが判明した製品を更新しました。	—	Final	2018年4月17日
1.4	IOS Software Checker にて、脆弱でないことが判明した製品を更新しました。	—	Final	2018年4月16日
1.3	デフォルトで Smart Install が有効であることを強調Smart Install をサポートするデバイスの一覧にリンクを追加	概要および該当製品	Final	2018年4月9日
1.2	「回避策」セクションに詳細を追加	回避策	Final	2018年

バージョン	説明	セクション	ステータス	日付
				4月6日
1.1	Metadata update.	—	Final	2018年4月2日
1.0	初回公開リリース	—	Final	2018年3月28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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。