Cisco Smart Install プロトコルの誤用

Inform ational

アドバイザリーID : cisco-sa-20170214-smi
初公開日 : 2017-02-14 00:00
最終更新日 : 2018-05-23 11:20
バージョン 4.2 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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 は、設定を完了した後、スマートなインストール機能がイネーブルになり、適切な緊急制御なしに残るデバイスを検出するように努めるインターネット スキャンの顕著な増加に気づいています。 これは機能の誤用するために複雑なデバイスを影響を受けやすいままにする可能性があります。 そうしなかった顧客は査定するこの表記の **推奨事項**セクションの指導に続くように勧められ、ネットワーク スイッチを確認するためにきちんとスマートなインストール機能の濫用から保護されます。

何人か研究者はスマートなインストール (SMI) プロトコル メッセージの使用でスマートなインストール クライアント、別名 *統合ブランチ クライアント (IBC)* の方に報告しま、 *startup-config* ファイルを変更し、デバイスのリロードを強制し、新しい IOS イメージをデバイスでロードし、Cisco IOS および IOS XE ソフトウェアが稼働しているスイッチの高特権 CLI コマンドを実行することを非認証、リモート攻撃者を許可します。
Cisco はこれを Cisco IOS、IOS XE、またはスマートなインストール機能自体認証を意図的に必要としないスマートなインストール プロトコルの誤用の脆弱性と考慮しませんが。 追求しているゼロ タッチ配備より多くを顧客は Ciscoネットワークをプラグ アンド プレイ ソリューション代りに展開することを考える必要があります。

Cisco は顧客 インフラストラクチャ内の Cisco スマートなインストール機能の配備に関するセキュリティ上の推奨事項を含むためにスマートなインストール コンフィギュレーション ガイドをアップデートしました。

これらの問題は維持可能なネットワーク セキュリティによって、デジタル セキュリティの Trustwave SpiderLabs のダニエル ターナー、およびアレキサンダー Evstigneev および Dmitry Kuznetsov 報告されました。

Cisco はスマートなインストール機能の濫用から最近スマートなインストールがイネーブルのままになったときに Cisco が公共ポストのことをこの機能の詳細潜在的な濫用学び、不正侵入のレポートを受け取ったので、ネットワーク スイッチを確認する必要についての顧客に警告するブログ ポストをきちんと保護されます送達してしまいました。 これらのブログ ポストは次のリンクで利用できます:

- Cisco PSIRT – Cisco スマートなインストール機能の潜在的な濫用を軽減し、検出します
- スマートなインストール クライアント プロトコル濫用のための Cisco カバレッジ

追加情報

Cisco スマートなインストール

Cisco スマートなインストールは新しい（一般的に アクセス層）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。 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 スイッチは直接ディレクターに接続される必要はありませんでしたり 7 つまでのホップである場合もあります。 スマートなインストール クライアントだけこの文書に説明がある誤用から影響を受けます切り替えます。

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 スイッチがネットワークに最初にインストールされているとき、ディレクターは自動的に新しいスイッチを検出し、ダウンロードのための正しい Cisco IOSイメージおよびコンフィギュレーション ファイルを識別します。 それはまたクライアントに IP アドレスおよびホスト名を割り当てることができます。

クライアント スイッチでは、Smart Install 機能はデフォルトで有効化されています。 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 Talos グループは顧客が環境で有効に なるスマートなインストール機能を備えているデバイスのためにスキャンするのに使用できるツールを発達させました。 このツールのさらに詳しい詳細については Talos ブログ ポストを参照して下さい。

スマートなインストール機能のより詳しい情報は スマートなインストール コンフィギュレーション ガイドで利用できます。

プロトコル誤用機会

クライアントとディレクター間のスマートなインストール プロトコルの許可または認証機構の不在はこれらのメッセージがスマートなインストール ディレクターから処理しあった、それらと同じような次のリストで操作をことができますようにクライアントが巧妙に細工された SMI プロトコル メッセージを行うことを可能にする:

- IBC の TFTPサーバアドレスを変更して下さい
- IBC から攻撃者制御 TFTPサーバに任意[1] ファイルをコピーして下さい
- 攻撃者が準備した代わりにし、明確な時間 間隔の後で IBC の読み込みを強制して下さいファイルが付いているクライアントの *startup-config* ファイルを
- IBC に攻撃者供給された IOS イメージをロードして下さい
- *exec* CLI コマンドを含む IBC の高特権 設定 モード CLI コマンドを、実行して下さい。 コマンド実行に出力のか敏速な起因は IBC のローカル コンソールで現われます (これは IOS 15.2(2)E および以降、および IOS XE 3.6.0E および以降だけで可能性のあるです)

IOS または IOS XE CLI の規則的な **copy コマンド**によってアクセスすることができるファイル システムからの [1 つの]ファイル。

推奨事項

Cisco スマートなインストール機能のまわりのセキュリティ上の推奨事項は機能が特定の顧客の環境で使用されるかによって決まります。 以降のセクションはユース ケースのそれぞれに指導を提供します。

スマートなインストール機能を使用する顧客ない

Cisco スマートなインストール機能を使用しない、コマンドが利用できる Cisco IOS または Cisco IOS XE ソフトウェアのリリースを実行している顧客は、 **vstack** 構成コマンドでスマートなインストール機能を (クライアントかディレクター) 無効に する必要があり。

次の例は有効に なるスマートなインストール クライアント機能が付いている Cisco Catalyst スイッチで **show vstack config** コマンドの出力を示します; これらはスマートなインストール クライアント機能は有効に なることを示す唯一の出力です:

```
switch1#show vstack config
Role: Client
.
.
.

switch2#show vstack config
Role: Client (SmartInstall enabled)
.
.
.

switch3#show vstack config
Capability: Client
```

```
Oper Mode: Enabled
    Role: Client
     .
     .
     .
```

注: スマートなインストール クライアント機能を Cisco 問題 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無効に する **vstack** グローバル な構成コマンドの使用は 4786）締める能力導入されませんでした。 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 問題 CSCtj75729 のための修正が含まれていません。

vstack コマンドが利用できないネットワークに関しては、「ゼロ タッチ配備より多くのためのスマートなインストール機能を」利用している顧客 セクションを参照して下さい。

注: vstack コマンドは Cisco IOS および IOS XE（この問題はディレクターだけとして機能できる）サポートの次のリリースで Cisco 問題 CSCvd99197 による読み込みを渡ってハードウェアプラットフォームだけの下にプラットフォーム依存しない、リリースの複数であり持続しませんではない。

- 12.2(60)EZ11
- 15.1(2)SY11
- 15.2(1)SY5
- 15.2(2)SY3
- 15.2(5)E2、15.2(5)E2a、15.2(5)E2b
- 15.4(1)SY3
- 3.9.2E、3.9.2aE、3.9.2bE

のこれらのリリース実行する場合、Cisco は非影響を受けたリリースか置かれたオートメーションにデバイスの各読み込みの後で **vstack** コマンドを再構成しないためにことをアップグレードまたはダウングレード推奨します。

ゼロ タッチ配備のためのスマートなインストール機能を全く利用している顧客

ゼロ タッチ配備のためのスマートなインストール機能を全く利用している顧客は **vstack** 構成コマンドでスマートなインストール機能を無効に する必要があります一度ずっとスイッチが配備されている。 **vstack** コマンドに関する更に詳しい情報については「スマートなインストール機能を使用して顧客ない」セクションを参照しないで下さい。

ゼロ タッチ配備より多くのためのスマートなインストール機能を利用している顧客

vstack コマンドが利用できないところでゼロ タッチ配備より多くのための Cisco スマートなインストール機能を利用している顧客は IBD だけポート 4786 のすべての IBCs に TCP 接続があることを確認し。 管理者は、影響を受けるデバイスでの Cisco Smart Install の導入に関する以下のセキュリティ ベスト プラクティスを使用することができます。

- インターフェイス アクセス コントロール リスト（ACL）
- コントロール プレーン ポリシング（CoPP はすべての Cisco IOS ソフトウェア リリースで

利用できません）

インターフェイス ACL は 10.10.10.1 であるスマートなインストール ディレクターの IP アドレスおよび 10.10.10.200 であるスマートなインストール クライアントの IP アドレスの次の例のように、見えるかもしれません:

```
    switch3#show vstack config
Capability: Client
Oper Mode: Enabled
    Role: Client
    .
    .
    .
```

この ACL は、すべての IBC のすべての IP インターフェイスに展開する必要があります。 先にスイッチを展開すると、IBD を介してプッシュできます。

更にインフラストラクチャ 管理者内のすべての IBCs へのアクセスを制限することはネットワークで他のデバイスの次のセキュリティ上の推奨事項を使用できます:

- インフラストラクチャ アクセスコントロール アクセス・コントロール・リスト（iACLs）
- VLAN アクセスコントロール アクセス・コントロール・リスト（VACL）

ネットワークの on Cisco 配置されたデバイス、iACLs および VACL を含んでである場合もある追加軽減についての情報に関しては次の場所で利用可能である Cisco IOS ソフトウェア スマートなインストール脆弱性のための Denial of Service（DoS/DDoS） 以前に送達された Cisco によって加えられる軽減情報（AMB）ドキュメントガイドを参照して下さい、:
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20120328-smartinstall

セキュリティ侵害の痕跡

スマートなインストール機能を使用してデバイスを離れて TFTPサーバアドレスをまたは攻撃者単なるファイルのインジケーターが変更する攻撃者ありません。 Cisco は顧客が外部 IP アドレスからアクセスを探すことを推奨します。

書き込み操作がスマートなインストール機能によって誘導され、ログ レベルが 6 にメッセージがログに現れれば（ *情報*）またはより高い設定 されれば。

startup-config が取り替えられる場合、次のメッセージは影響を受けたデバイスからのログで一般的に見られます:

```
    switch3#show vstack config
Capability: Client
Oper Mode: Enabled
    Role: Client
    .
    .
    .
```

設定 モードの高特権コマンドの実行は、スマートなインストール機能によって影響を受けたデバ

イスにログで作成される次のメッセージという結果に、一般的に終ります:

```
    switch3#show vstack config
Capability: Client
Oper Mode: Enabled
    Role: Client
    .
    .
    .
```

読み込みがスマートなインストール機能によって誘導され、ログ レベルが **5** に（ *通知* ）または より高い設定 されれば、次のメッセージの 1 つがログに現われれば:

```
    switch3#show vstack config
Capability: Client
Oper Mode: Enabled
    Role: Client
    .
    .
    .
```

ローカルに加えてクライアントを切り替えますログオンし、クライアント スイッチが syslog サーバに送信 するログはまたファイアウォール ログおよび NetFlow データ、顧客調べる必要があります。

Cisco はカスタマ ネットワークのスマートなインストール プロトコル メッセージの使用の検出を助ける侵入防御システム（IPS）シグニチャ ID 7856-0、また Snort ルールを 41722-41725 送達しました。 Snort ルールの詳細については Talos ブログ ポストを参照して下さい。

false positive を避けるために、このシグニチャおよび Snort ルールはスマートなインストール機能を使用してまたはスマートなインストール プロトコル メッセージが見られると期待されないネットワークの場所でネットワークでだけない有効に する必要があります。

次の最良の方法はまたお勧めの 環境の可能性のある アノーマリにより多くの表示を提供するのに使用する必要がありますです:

- ネットワーク デバイスを監督し、交通モニタリング（テレメトリー ベースのインフラストラクチャ デバイス 統合 モニタリング）を有効に するために高価なネットワーク セグメント、デバイスおよびユーザーに焦点を当てられる補足実装の実装
- 期待されたトラフィックに対して評価のためのネットワークの各部分から出るトラフィック フローへの表示用の Cisco IOS NetFlow の実装
- ネットワーク デバイス イベント ログの予想外ネットワーク デバイスレベル アクティビティを識別するためにモニタ

追加最良の方法に関しては、 Cisco IOSデバイスおよび Cisco IOSイメージ 確認 白書を 堅くするために Cisco ガイドを参照して下さい。

Ciscoセキュリティ手順

セキュリティ上の問題の支援を得、Cisco からセキュリティ情報を受け取るために登録するシス

コ製品のレポート セキュリティーの脆弱性の完全情報は http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html で Cisco Worldwide Web サイトで利用できます。 これには手順がのための押します Ciscoのセキュリティの告知に関する照会を含まれています。 すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi

改訂履歴

Version	Description	Section	Status	日付
4.2	CSCvd99197 のための更新済該当製品およびバージョン-「vstack」は読み込みを渡って、持続しません。	推奨事項	Final	2018-May-23
4.1	それが SMI をサポートしないので Catalyst 6500 が SMI ディレクター機能だけサポートすること明白になる ME 3400 および ME 3400E についての更新済 show vstack config 出力、取除かれた情報。	推奨事項		2018 年 4 月 16 日
4.0	高められた公開に関するアップデート、CSCvd99197 に付け加えられたメモ。	Cisco 応答、推奨事項		2017-October-30
3.0	任意ファイルおよびログ メッセージをコピーする可能性に関する更新。	プロトコル誤用機会、侵害のインジケーター		2017-March-03
2.1	clarified デバイス出力に影響を与えました。	推奨事項		2017-March-01
2.0	公共濫用に関する更新。	â		2017-February-27
1.0	初期リリース。			2017-February-14

利用規約