Cisco IOSおよびIOS XEソフトウェアのSM-1T3/E3 Service ModuleにおけるDoS脆弱性

High

アドバイザリーID : cisco-sa-20180926-sm1t3e3
初公開日 : 2018-09-26 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco バグ ID : CSCvi95007 CSCva23932

CVE-2018-0485

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 第 2 世代サービス統合型ルータ (ISR G2) および Cisco 4451 X Integrated Services Router (ISR4451 X) で SM-1T3/E3 ファームウェアの脆弱性により、ISR G2 ルータや SM 1T3/E3 原因となる、認証されていない、リモートの攻撃者モジュールはリロードする ISR4451 X の影響を受けるデバイスで (DoS) 状態 Denial of Service (DoS) で発生します。

攻撃者は、SM-1T3/E3 モジュールのコンソールに接続する最初の文字列のシーケンスを入力し、この脆弱性を悪用する可能性があります。成功したエクスプロイト攻撃者があります。 ISR G2 ルータまたは SM-1T3/E3 モジュールをリロードする ISR4451 X の原因に影響を受けるデバイスで DoS 状態になります。

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。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-sm1t3e3

このアドバイザリは、2018 年 9 月 26 日に公開された 13 件の脆弱性に関する 12 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 アドバイザリ公開資料の一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 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

Cisco SM-X-1T3/E3 1 ポート T3/E3 拡張サービス モジュール (SM X) は、Cisco ISR G2 および Cisco ISR4451 X のルータでサポートされているソフトウェア設定可能な T3/E3 製品です。

脆弱性のある製品

この脆弱性に影響を与える Cisco ISR G2 または Cisco ISR4451 X ルータ SM-X-1T3/E3 モジュールがあるかどうかがインストールされているし、影響を受けるバージョンの Cisco IOS または IOS XE ソフトウェアを実行しています。

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。

SM-X-1T3/E3 モジュールがインストールされているかどうかを決定します。

Cisco ISR G2 ルータで次のように入力します。、 バージョンの show CLI コマンド。出力が含まれている場合 Subrate T3/E3 ポート 、デバイスがある影響を受けるモジュールがインストールされています。次の例では、インストールされている SM X-1T3 E3/モジュールと、デバイスを示します。

```
<#root>

ISR-G2#

show version | include T3/E3

1

Subrate T3/E3 port

ISR-G2#
```

出力は、何も返された場合、デバイスには、SM-X-1T3/E3 モジュールの取り付け項目がありません。

ISR4451 X ルータでは、入力、 すべて eeprom 診断の表示 | SM-X-1T3 を含める CLI コマンド。出力が含まれている場合 SM-X-1T3/E3 、デバイスがある影響を受けるモジュールがインストールされています。次の例では、インストールされている SM X-1T3 E3/モジュールと、デバイスを示します。

```
<#root>

ISR-G2#

sho diag all eeprom | include SM-X-1T3
```

```
Product Identifier (PID) : SM-X-1T3/E3

ISR-G2#
```

出力は、何も返された場合、デバイスには、SM-X-1T3/E3 モジュールの取り付け項目がありません。

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

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

詳細

SM-X-1T3/E3 モジュールのファームウェアは Cisco IOS または IOS XE ソフトウェア イメージ内でバンドルされています。

SM-X-1T3/E3 コンソール

ユーザに SM-X-1T3/E3 コンソールにセッションがある場合にのみこの脆弱性が悪用です。

Cisco Bug ID より前の ISR G2 ルータで CSCuz92665 、SM-X-1T3/E3 コンソールが TTY 回線の設定に基づいてリモートからアクセスできます。参照してください、 の回避策 セクション SM-X-1T3/E3 コンソールへのリモート アクセスを防止する設定を変更します。ISR G2 ルータでローカル認証を使用している場合、回線が認証なしでアクセス可能な可能性があります。認証、認可、アカウンティングを使用している場合に、モジュールをリモートでアクセス (AAA) 認証、有効なユーザ名とパスワードの組み合わせが必要です。

ISR4451 X ルータ SM-X-1T3/E3 コンソールで、のみ使用可能な privilege 15 を使用したローカル

な # hw-module セッション <slot ard=""> コマンド</slot>。

ISR G2 ルータでは、脆弱性が悪用するとには、全体のルータをリロードします。

ISR4451 X ルータでは、SM-X-1T3/E3 モジュールだけがリロードされます。

両方のデバイスで SM-X-1T3/E3 モジュール 180 秒以上のされます。

固定ソフトウェアのリリースでは、ISR G2 ルータのみへのアップグレード

ISR G2 ルータでの固定ソフトウェアリリースにアップグレードする前に、デバイス上の既存のファームウェアを削除します。次の CLI 出力は、該当するコマンドの例を示します。

```
ISR-G2#delete flash0:/firmware/sm_1t3e3/sm_1t3e3_fw.ver
Delete filename [/firmware/sm_1t3e3/sm_1t3e3_fw.ver]?
Delete flash0:/firmware/sm_1t3e3/sm_1t3e3_fw.ver? [confirm]
ISR-G2#
ISR-G2#delete flash0:/firmware/sm_1t3e3/sm_1t3e3_fw.img
Delete filename [/firmware/sm_1t3e3/sm_1t3e3_fw.img]?
Delete flash0:/firmware/sm_1t3e3/sm_1t3e3_fw.img? [confirm]
ISR-G2#
```

回避策

脆弱性のエクスプロイトができない場合は、次の回避策が、攻撃対象領域を制限するは。

SM-X-1T3/E3 コンソール (ISR G2 ルータのみ) にアクセスできなくなります。

SM-X-1T3/E3 コンソールへのアクセスがの設定によって無効にすることをお勧め transport input none 次の例のよ SM-X-1T3/E3 コンソールに関連付けられている回線で。

<#root>

```
ISR-G2#configure terminal
ISR-G2(config)#line 68
ISR-G2(config)#
transport input none
ISR-G2(config)#exit
ISR-G2#
```

Cisco ISR4451 X ルータ、SM-X-1T3/E3 コンソールにはのみ使用可能な privilege 15 を使用したローカルな # hw-module セッション <slot ard=""> コマンド</slot>

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

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間（Medium）] チェックボックスをオンにします。

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）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

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-20180926-sm1t3e3

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2018 年 9 月 26 日

利用規約

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。