Cisco IOS および IOS XE ソフトウェアの Session Initiation Protocol で確認されたサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20190925-sip-dos

初公開日 : 2019-09-25 16:00

最終更新日 : 2019-10-04 22:21

バージョン 1.1 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvn00218

CVE-2019-12654

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 Session Initiation Protocol（SIP）共有ライブラリで脆弱性が確認されました。認証されていないリモートからの攻撃者によって、標的デバイスのリロードが引き起こされ、その結果、サービス妨害（DoS）状態に陥る危険性があります。

この脆弱性は、内部データ構造の健全性チェックが不十分であることに起因します。 標的デバイスに一連の悪意のある SIP メッセージを送信することで、エクスプロイトされる可能性があります。 エクスプロイトによって、ヌル ポインタの逆参照が可能になるため、 *iosd* プロセスのクラッシュに繋がる危険性があります。 クラッシュが発生すると、デバイスのリロードが引き起こされます。

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ました。 この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-sip-dos

このアドバイザリは、2019 年 9 月 25 日に公開された Cisco IOS および IOS XE ソフトウェア リリースのセキュリティ アドバイザリ資料の一部です。この資料には、13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリが記載されています。 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、2019 年 9 月）

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、シスコ ルータで脆弱性のある Cisco IOS または IOS XE ソフトウェアを稼動しており、次の機能のいずれかが有効になっている場合です。

- Cisco Unified Border Element（CUBE）
- Cisco Unified Communications Manager Express（CME）
- Cisco IOS Gateways with Session Initiation Protocol（SIP）
- Cisco TDM ゲートウェイ
- Cisco Unified Survivable Remote Site Telephony（SRST）
- Cisco Business Edition 4000（BE4K）

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の詳細は、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。

デバイスの脆弱性の確認

デバイスに脆弱性があるかどうかを確認するには、管理者が **show processes | include CCSIP_SPI_CONTRO** コマンドを CLI で実行して、*CCSIP_SPI_CONTRO* プロセスがあるかを確認します。 以下は、対象機能の少なくとも 1 つが有効になっているデバイスで **show processes | include CCSIP_SPI_CONTRO** コマンドを実行した場合の出力例です。このような場合、脆弱性があります。

```
Router#show processes | include CCSIP_SPI_CONTRO
 671 Mwe 561F108FE8BA            10         11     909234584/240000  0 CCSIP_SPI_CONTRO
```

このコマンドによる出力がない場合は、対象の機能が有効になっていないため、そのデバイスには脆弱性がありません。

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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成功すると、該当するデバイスがリロードされ、crashinfo ファイルが生成されます。

この脆弱性が不正利用されているかどうかを確認するには、デバイスのスタック トレースをデコードして、スタック トレースと本脆弱性との関連性を確認します。

crashinfo ファイルを確認し、デバイスにこの脆弱性の不正利用が発生していないかを判別するには、Cisco Technical Assistance Center（TAC）までご連絡ください。

回避策

この脆弱性に対処する回避策はありません。

だれが有効に なる リリース 16.11 前に自動的に Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェア リリースの SIP プロセスを有効に する他の音声関係 機能があるか SIP 機能を使用しないが、SIP ポートをシャットダウンできます顧客はグローバル コンフィギュレーション モードの次のコマンドの発行によって:

```
Router(config)#sip-ua
Router(config-sip-ua)#no transport udp
Router(config-sip-ua)#no transport tcp
Router(config-sip-ua)#no transport tcp tls
```

また、顧客は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）を使用して指定 SIP ポートに目標とされるトラフィックをブロックできます。 iACLs を使用するネットワーク セキュリティ 最良の方法はあり、よいネットワーク セキュリティへの長期付加、またこの特定の問題のための軽減として考慮する必要があります。 インフラストラクチャ IPアドレス範囲の IP アドレスのすべてのデバイスの保護を助けるために顧客は展開された iACL の一部として次の iACL 例を含むように勧告されます:

```
!---
!--- Feature: SIP
!---

!---
!--- Deny SIP traffic from all other sources destined
!--- to infrastructure addresses
!---

access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 5060
access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 5060
access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 5061

!---
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.
!---

access-list 150 permit ip any any

!---
!--- Apply access-list to all interfaces (only one example
```

```
!--- shown)
!---

interface GigabitEthernet 2/0
 ip access-group 150 in
```

iACLs の配備手法のそれ以上のガイドラインおよび推奨事項に関しては、白書をコアを保護することを参照して下さい: インフラストラクチャ 保護 アクセス コントロール リスト（ACL）および Cisco IOSデバイスを堅くする Cisco ガイド。

注: デフォルトで、SIP は SIP のために UDP および TCPポート 5060 および TLS 上の SIP のために TCPポート 5061 を使用します。 ただし、これらのポートは **音声サービス voip > ー**ロコンフィギュレーションモードのリッスン **ポート非セキュア** *<port_number>* およびリッスン **ポートセキュア** *<port_number>* コマンドを使用してユーザ側で設定できます。 カスタム SIP ポートが設定される場合、前例 iACL の UDP および TCP ポートはそれに応じて調節される必要があります。

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。
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、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 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

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、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。

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）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、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-sip-dos

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	追加された軽減 オプション。	回避策	最終版	2019-October-04
1.0	初回公開リリース		最終版	2019 年 9 月 25 日

利用規約