Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability

Advisory ID: cisco-sa-20131106-sip

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131106-sip

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。

Revision 1.0

For Public Release 2013 November 6 16:00 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアにおける Session Initiation Protocol（SIP; セッション開始プロトコル）の実装には脆弱性が存在します。このため、認証されていないリモートの攻撃者によって該当するデバイスの再起動またはメモリ リークが引き起こされ、システムが不安定になることがあります。この脆弱性を不正利用するには、SIP メッセージを処理するように該当デバイスが設定されている必要があります。影響を受ける Cisco IOS ソフトウェア リリースは限定的です。

シスコはこの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ました。

SIP を実行する必要のあるデバイスについては回避策がありません。ただし、脆弱性の発現を軽減することはできます。

このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131106-sip

該当製品

脆弱性が認められる製品

影響を受けるシスコ デバイスは、SIP メッセージを処理するように設定されている該当 IOS ソフトウェア リリースを実行しているデバイスです。次の Cisco IOS ソフトウェアが、この脆弱性の影響を受けます。

- 15.1(4)GC および 15.1(4)GC1
- 15.1(4)M4、15.1(4)M5、および 15.1(4)M6

Cisco IOS ソフトウェアの最近のリリースでは、デフォルトでは SIP メッセージが処理されません。 **dial-peer voice** コンフィギュレーション コマンドによるダイヤル ピアの作成によって SIP プロセスが開始されることで、Cisco IOS デバイスは SIP メッセージの処理を行います。さらに、Cisco Unified Communications Manager Express の一部の機能（ePhone など）が設定されると自動的に SIP プロセスが開始され、デバイスによる SIP メッセージの処理が開始されます。該当する設定の例は次のとおりです。

```
!
dial-peer voice <Voice dial-peer tag> voip
...
!
```

管理者は、SIP メッセージを処理する **dial-peer** コマンドが Cisco IOS デバイスの設定にないか調べることに加えて、 **show processes | include SIP** コマンドを使用することにより、Cisco IOS ソフトウェアが SIP メッセージを処理するプロセスを実行しているかどうかを判断することができます。次の例では、CCSIP_UDP_SOCKET または CCSIP_TCP_SOCKET のプロセスが表示されているため、Cisco IOS デバイスが SIP メッセージを処理することがわかります。

```
Router# show processes | include SIP
 149 Mwe 40F48254            4          1    400023108/24000  0
CCSIP_UDP_SOCKET
 150 Mwe 40F48034            4          1    400023388/24000  0
CCSIP_TCP_SOCKET
```

注：Cisco IOS ソフトウェアを実行しているデバイスで、SIP メッセージの処理を開始する方法は複数存在します。そのため、デバイスが SIP メッセージを処理しているかどうかを判断するには、特定のコマンドが設定されているかどうかではなく、 **show processes | include SIP** コマンドを使用することを推奨します。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインし **show version** コマンドを実行してシステム バナーを表示させます。「Internetwork Operating System Software」、「Cisco IOS Software」あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。その後ろにイメージ名が括弧の間に表示され、続いてバージョンと Cisco IOS ソフトウェア リリース名が表示されます。他のシスコ デバイスでは、 **show version** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.0(1)M1 が稼働し、インストールされているイメージ名が C3900-UNIVERSALK9-M であることを示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version
15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
!-- output truncated
```

Cisco IOS ソフトウェアのリリース命名規則の追加情報は、以下のリンクにある「White Paper: Cisco IOS and NX-OS Software Reference Guide」で確認できます。

http://www.cisco.com/web/about/security/intelligence/ios-ref.html

脆弱性が認められない製品

Cisco IOS XE ソフトウェアおよび Cisco Unified Communications Manager は、この脆弱性の影響を受けません。この脆弱性の影響を受ける他のシスコ製品は、現在確認されていません。

詳細

SIP は一般的なシグナリング プロトコルであり、インターネットなどの IP ネットワークで音声およびビデオ コールの管理に使用されます。SIP はコールのセットアップと終了に関するすべてを処理します。SIP で処理される最も一般的なセッション タイプは音声とビデオですが、SIP はコールのセットアップと終了を必要とするその他のアプリケーションにも柔軟に対応します。SIP コール シグナリングでは、転送プロトコルとして UDP ポート 5060、TCP ポート 5060、または Transport Layer Security（TLS）（TCPポート 5061）を使用します。

Cisco IOS ソフトウェアのセッション開始プロトコルの機能に存在する脆弱性により、認証されていないリモートの攻撃者が、メモリ リークまたはデバイスの再起動を引き起こす可能性があります。

この脆弱性は、巧妙に細工された SIP メッセージの誤処理に起因します。攻撃者は、特定の有効な SIP メッセージを SIP ゲートウェイに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。不正利用によって、攻撃者はメモリ リークまたはデバイスの再起動を引き起こすことができます。

この脆弱性は、Cisco IOS ソフトウェアを実行するデバイスが特定の有効な SIP メッセージを処理すると引き起こされます。この脆弱性は、デバイス宛てのトラフィックよってのみ引き起こされます。デバイスを通過する SIP トラフィックによって脆弱性が引き起こされることはありません。IPv4 または IPv6 通信プロトコルで SIP を実行している場合に、この脆弱性を不正利用できます。

注：SIP が TCP トランスポートで実行されている場合、この脆弱性を不正利用するには TCP 3 ウェイ ハンドシェイクが必要です。

この脆弱性は、Cisco bug ID CSCuc42558（ 登録ユーザ専用）および CSCug25383（ 登録ユーザ専用）として文書化されています。この脆弱性に対して Common Vulnerabilities and Exposures（CVE）ID CVE-2013-5553 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。
http://tools.cisco.com/security/center/cvssCalculator.x/

CSCuc42558 and CSCug25383 - Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

本アドバイザリに記載された脆弱性の不正利用に成功した場合、システムが不安定になったり、影響を受けるデバイスの再起動が発生したりすることがあります。繰り返し悪用されると、サービス拒否（DoS）状態が続く可能性があります。

ソフトウェア バージョンおよび修正

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

Cisco IOS ソフトウェア

Cisco IOS ソフトウェア テーブル（下記）の各行は Cisco IOS ソフトウェア トレインを示します。あるトレインが脆弱性を含む場合、修正を含む最初のリリースは「First Fixed Release」列に示されます。シスコは利用可能な最新のリリースへのアップグレードを推奨します。

Cisco IOS ソフトウェア チェッカーを利用して、特定の Cisco IOS ソフトウェア リリースに対応したシスコのセキュリティ アドバイザリを検索することができます。このツールは次の Cisco Security Intelligence Operations（SIO）ポータルで利用できます。
http://tools.cisco.com/security/center/selectIOSVersion.x

Major Release	Availability of Repaired Releases

Affected 12.0-Based Releases	First Fixed Release
There are no affected 12.0 based releases	
Affected 12.2-Based Releases	First Fixed Release
There are no affected 12.2 based releases	
Affected 12.3-Based Releases	First Fixed Release
There are no affected 12.3 based releases	
Affected 12.4-Based Releases	First Fixed Release
There are no affected 12.4 based releases	
Affected 15.0-Based Releases	First Fixed Release
There are no affected 15.0 based releases	
Affected 15.1-Based Releases	First Fixed Release
15.1EY	Not vulnerable
15.1GC	Vulnerable; first fixed in release 15.1M Releases prior to 15.1(2)GC2 are not affected.
15.1M	15.1(4)M7 Releases prior to 15.1(4)M4 are not affected.
15.1MR	Not vulnerable
15.1S	Not vulnerable
15.1SG	Not vulnerable
15.1SNG	Not vulnerable
15.1SNH	Not vulnerable
15.1T	Not vulnerable
Affected 15.2-Based Releases	First Fixed Release
There are no affected 15.2 based releases	
Affected 15.3-Based Releases	First Fixed Release
There are no affected 15.3 based releases	

回避策

該当する Cisco IOS デバイスで VoIP サービスを行っていて SIP をディセーブルにできない場合、回避策はありません。この脆弱性の発現を最小限に抑えるため、緩和策を適用することを推奨します。対応策とは、正当なデバイスだけがデバイスに接続できるように設定することです。効果を高めるには、この緩和策をネットワーク エッジにおけるアンチスプーフィングと組み合わせて利用する必要があります。この処理が必要になるのは、SIP の転送プロトコルとして UDP も使用できるためです。

ネットワーク内のシスコ デバイスに適用可能なその他の回避策については、付属ドキュメント「Identifying and Mitigating Exploitation of the Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability」で紹介しています。このドキュメントは、次のリンクから入手可能です。 http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=31516

SIP リスニング ポートのディセーブル化

SIP をイネーブルにする必要がないデバイスの場合、最も簡単かつ効果的な回避策はそのデバイスの SIP 処理をディセーブルにすることです。Cisco IOS ソフトウェアの一部のリリースでは、管理者が次のコマンドを使用して SIP をディセーブルにすることができます。

```
sip-ua
no transport udp
no transport tcp
no transport tcp tls
```

警告：この回避策をメディア ゲートウェイ コントロール プロトコル（MGCP）または H.323 コールを処理しているデバイスに適用すると、アクティブ コールの処理中は SIP の処理が停止されません。このような場合は、アクティブ コールを一時的に停止できるよう、メンテナンス時にこの回避策を実行します。

show udp connections コマンド、 **show tcp brief all** コマンド、および **show processes | include SIP** コマンドを使用すれば、この回避策を適用した後に SIP UDP ポートおよび TCP ポートが閉じていることを確認できます。

使用中の Cisco IOS ソフトウェア リリースによっては、SIP がディセーブルにされたとき、**show ip sockets** コマンドコマンドの出力でまだ SIP ポートが開かれていると表示されることがありますが、それらにトラフィックを送信すると SIP プロセスは次のメッセージを表示します。

```
*Nov 2 11:36:47.691: sip_udp_sock_process_read: SIP UDP Listener is
DISABLED
```

コントロール プレーン ポリシング

SIP サービスが必要なデバイスの場合は、Control Plane Policing（CoPP）を使用して、信頼できない発信元からの SIP トラフィックをブロックできます。CoPP 機能は、Cisco IOS ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T でサポートされています。管理およびコントロール プレーンを保護するために CoPP をデバイスに設定し、既存のセキュリティ ポリシーとコンフィギュレーションに従って認定されたトラフィックだけがインフラストラクチャ デバイス宛に送信されることを明示的に許可することで、インフラストラクチャへの直接攻撃のリスクとその効果を最小限に抑えることができます。次の例は、特定のネットワーク設定に適用できます。

```
!- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!- Everything else is not trusted. The following access list is used
!- to determine what traffic needs to be dropped by a control plane
!- policy (the CoPP feature): if the access list matches (permit)
!- then traffic will be dropped and if the access list does not
!- match (deny) then traffic will be processed by the router.
access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060 access-list 100
deny tcp 192.168.1.0 0.0.0.255 any eq 5060 access-list 100 deny tcp
192.168.1.0 0.0.0.255 any eq 5061 access-list 100 deny udp host 172.16.1.1
any eq 5060 access-list 100 deny tcp host 172.16.1.1 any eq 5060 access-
list 100 deny tcp host 172.16.1.1 any eq 5061 access-list 100 permit udp
any any eq 5060 access-list 100 permit tcp any any eq 5060 access-list 100
permit tcp any any eq 5061
!- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4 !-
traffic in accordance with existing security policies and !- configurations
for traffic that is authorized to be sent !- to infrastructure devices. !-
Create a Class-Map for traffic to be policed by !- the CoPP feature.
class-map match-all drop-sip-class match access-group 100
!- Create a Policy-Map that will be applied to the !- Control-Plane of the
device.
policy-map control-plane-policy class drop-sip-class drop
!- Apply the Policy-Map to the Control-Plane of the !- device. control-
plane service-policy input control-plane-policy
```

注：SIP は転送プロトコルとして UDP も使用できるため、IP パケットの送信元アドレスを詐称して、信用された IP アドレスからのこれらポート宛の通信を許可する ACL を回避される可能性があります。ユニキャスト リバース パス転送についての追加情報は、次のリンクで確認できます。 http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html

上記の CoPP の例では、「permit」アクションによってアクセス コントロール リスト エントリ（ACE）に該当し、攻撃である可能性のあるパケットは、policy-map の「drop」機能により廃棄されますが、一方、「deny」アクション（記載されていません）に該当するパケットは、policy-map の「drop」機能の影響を受けません。CoPP の設定と使用方法についての追加情報は、次のリンクで確認できます。 http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html および http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

修正済みソフトウェアの入手

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。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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、ご購入いただいたフィーチャ 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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレードを入手することができます。 http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- Eメール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）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不正利用事例とその公表は確認しておりません。

この脆弱性は、お客様からのサービス要求の処理中にシスコが発見したものです。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131106-sip

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2013-November-06	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。