SIPパケットがSIPをサポートするIOSデバイスをリロードする

アドバイザリーID : cisco-sa-20070131-sip CVE-2007-0648
初公開日 : 2007-01-31 00:00
バージョン 2.1 : Final
CVSSスコア : 3.3
回避策 : No Workarounds available
Cisco バグ ID : CSCsb25337 CSCsh58082

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

Session Initiation Protocol（SIP；セッション開始プロトコル）をサポートする該当バージョンのInternetwork Operating System(IOS)が稼働しているシスコデバイスは、ポート5060宛ての特定の一連のパケットを受信する際にデバイスのリロードを引き起こす可能性のある脆弱性の影響を受けます。この問題は、SIPが設定されていないデバイスでTCP 5060およびUDPポート5060へのトラフィックを許可する関連バグによって悪化します。

この問題が意図的に悪用された例は報告されていません。ただし、この脆弱性を偶然に誘発したものと思われるデータ ストリームは観察されています。

SIPを必要としないデバイスに対するこの問題の影響を緩和する回避策があります。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070131-sip で公開されています。

該当製品

脆弱性のある製品

脆弱性が存在するバージョンのIOSを実行し、SIP処理をサポートするシスコデバイスには、脆弱性が存在する可能性があります。これには、IOSバージョン12.3(4)XH、12.3(4)XQ、12.3(7)XR、12.3(7)XS、12.3(8)JA、12.3(8)T、12.3(8)XU、12.3(8)XW、12.3(8)XX、12.3(8)XY、12.3(8)YA、12.3(8)YAが8 YG、12.3(8)YH、12.3(8)YI、12.3(8)ZA、12.4メインライン、および12.4T以降。SIP公衆電話交換網(PSTN)ゲートウェイとして設定されているルータや、SIPセッションボーダーコントローラ(SBC)およびCAT6000-CMMカードとして設定され

ているルータには脆弱性が存在します。

デバイスでSIPが有効になっているかどうかを確認するには、show ip socketsコマンドとshow tcp brief allコマンドを入力します。次に、修正も回避策も有効にせずにコードを実行しているルータの例を示します。この例のルータでは、脆弱性のあるイメージc7200-p-mz.124-3.binが実行されています。

```
<#root>

Router#

show ip sockets

Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
17 0.0.0.0             0  --any--          5060   0   0  211   0
17 0.0.0.0             0 192.168.100.2       67   0   0 2211   0
17 0.0.0.0             0 192.168.100.2     2517   0   0   11   0
```

UDP SIP が有効であることは、UDP ポート 5060 を含む最初の行によって示されます。

```
<#root>

Router#

show tcp brief all

TCB       Local Address           Foreign Address        (state)
2051E680  *.5060                  *.*                    LISTEN
```

TCP SIP が有効であることは、*.5060 を含む行によって示されます。

脆弱性を含んでいないことが確認された製品

SIP処理をサポートしていないデバイスは、この問題の影響を受けません。これには、6500、7600、10000シリーズおよび12000シリーズが含まれますが、これらに限定されません。デバイスにこの問題の脆弱性がないことを確認するには、show tcp brief allコマンドとshow ip socketsコマンドを使用して、TCP 5060とUDP 5060のポートがデバイスで開いていないことを確認します。次に、この問題に対して脆弱ではない固定イメージc7200-js-mz.124-5b.binを実行しているルータの例を示します。

```
<#root>

Router#

show tcp brief all
```

```
Router#

show ip sockets

Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
17 0.0.0.0             0 192.168.100.2      67   0   0 2211   0
```

UDPポート5060の行は表示されず、UDP SIPは有効になっていません。この例では、UDPポート67がこの脆弱性に関連しないDHCPによって使用されています。

詳細

SIPはIP音声ネットワークで使用するために設計されたプロトコルで、世界中のVoice over Internet Protocol(VoIP)通信で広く使用されています。

SIPサービスをサポートする特定のバージョンのIOSを実行しているシスコデバイスは、TCPポート5060またはUDPポート5060に巧妙に細工された一連のSIPパケットによってデバイスのリロードを引き起こす脆弱性の影響を受ける可能性があります。この脆弱性は、SIPゲートウェイなど、SIP設定を含むルータに影響を与えます。この問題は、Cisco Bug ID CSCsh58082(登録ユーザ専用)に記載されています。

さらに、SIPサービスをサポートする特定のバージョンのIOSでは、SIP動作が設定されていない場合でもSIPメッセージを処理する場合があります。SIPメッセージを処理するために、IOSはUDPポート5060およびTCPポート5060をリスニング用に開きます。SIP動作を設定せずにSIPメッセージを処理するIOSの問題について文書化されているCisco Bug IDは、CSCsb25337(登録ユーザ専用)です。このバグの修正により、リスニングポートTCP 5060およびUDP 5060がオフになります。

この問題に対して脆弱なデバイスは、SIPポートが開いている必要があります。TCP 5060またはUDP 5060でリッスンしないデバイスには脆弱性はありません。SIPはトランスポートとしてUDPを使用するため、送信元のIPアドレスをスプーフィングして、信頼できるIPアドレスからこれらのポートへの通信を許可するACLを無効にできる可能性があります。

回避策

ネットワーク内のCiscoデバイスに適用可能な他の対応策は、このアドバイザリに関連するCisco適用対応策速報(https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070131-sip)を参照してください。

SIPリスニングポートの無効化

SIPを有効にする必要がないデバイスに対する最も簡単で効果的な回避策は、次のコマンドを使用してデバイスのSIP処理を無効にすることです。

警告：この回避策を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にデバイスでSIP処理を停止できなくなります。このような状況では、この回避策は、アクティブコールを一時的に停止できるメンテナンスウィンドウ中に実装する必要があります。

<#root>

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
sip-ua
Router(config-sip-ua)#
no transport udp
Router(config-sip-ua)#
no transport tcp
Router(config-sip-ua)#
end
```

この回避策を適用すると、show ip socketsコマンドとshow tcp brief allコマンドでは、UDPおよびTCPポート5060でリスニングしているデバイスは表示されません。

<#root>

```
Router#
show ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY
 17   --listen--          9.13.32.18       2887   0   0   11   0
Router#
show tcp brief all
TCB       Local Address           Foreign Address        (state)
6649A5A4  *.1720                  *.*                    LISTEN
66CDC764  *.1723                  *.*                    LISTEN
```

コントロール プレーン ポリシング

SIPを実行する必要がないデバイスでは、コントロールプレーンポリシング(CoPP)を使用して、デバイスへのすべてのSIPアクセスをブロックできます。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 は、CoPP 機能をサポートしています。デバイスに CoPP を設定して、管理プレーンとコントロール プレーンを保護し、既存のセキュリテ

ィ ポリシーおよび設定に従って、インフラストラクチャのデバイスに送信される承認されたトラフィックだけ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効果を最小限に抑えることができます。次の例をネットワークに適用できます。

警告：SIPはトランスポートとしてUDPを使用するため、送信者のIPアドレスをスプーフィングして、信頼できるIPアドレスからこれらのポートへの通信を許可するACLを無効にできる可能性があります。

```
!-- Permit all TCP and UDP SIP traffic sent to all IP addresses
!-- configured on all interfaces of the affected device so that it
!-- will be policed and dropped by the CoPP feature.


access-list 100 permit tcp any any eq 5060
access-list 100 permit udp any any eq 5060


!-- 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 drop-sip-traffic
  class drop-sip-class
    drop


!-- Apply the Policy-Map to the Control-Plane of the
!-- device.


control-plane
  service-policy input drop-sip-traffic
```

上記のCoPPの例では、access control list entries（ACE；アクセスコントロールリストエントリ）の潜在的な悪用パケットに「permit」アクションが一致する場合、これらのパケットはポリシーマップの「drop」機能によって廃棄されますが、「deny」アクション（非表示）に一致するパ

ケットは、ポリシーマップのdrop機能の影響を受けません。CoPP 機能の設定と使用に関する詳細は、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd8 および http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html を参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、リリース トレインとそれに対応するプラットフォームまたは製品が記載されています。特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（「第 1 修正済みリリース」）とそれぞれの提供日が「リビルド」列と「メンテナンス」列に記載されます。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。このようなリリースは、少なくとも、示されているリリース以上（最初の修正リリース ラベル以上）にアップグレードしてする必要があります。

「リビルド」および「メンテナンス」という用語の詳細については、次のURLを参照してください。http://www.cisco.com/web/about/security/intelligence/ios-ref.html

次の表は、CSCsh58082(登録ユーザ専用)の脆弱性および修正済みステータスを示しています。これは、デバイスのリロードを引き起こすバグです。この表には、デバイスのSIP動作が完全に設定されていない場合にSIPメッセージの処理をオフにするCSCsb25337(登録ユーザ専用)に対して修正されたIOSリリースに関する情報も含まれています。2.0の公開時点では、CSCsh58082(登録ユーザ専用)に対する修正はありません。

メジャー リリース	修正済みリリースの入手可能性	
該当する 12.0 ベースのリリース	リビルド	メンテナンス

12.0	すべての12.0リリースには脆弱性はありません	
該当する 12.1 ベースのリリース	リビルド	メンテナンス
12.1	すべての12.1リリースには脆弱性はありません	
該当する 12.2 ベースのリリース	リビルド	メンテナンス
12.2	すべての12.2リリースには脆弱性はありません	
該当する 12.3 ベースのリリース	リビルド	メンテナンス
12.3	脆弱性なし	
12.3B	脆弱性なし	
12.3BC	脆弱性なし	
12.3BW	脆弱性なし	
12.3JA	脆弱性なし	
12.3JEA	脆弱性なし	

12.3JK	脆弱性なし
12.3JX	脆弱性なし
12.3T	12.3(8)T以降のすべてのリリースに脆弱性あり
12.3TPC	脆弱性なし
12.3XA	脆弱性なし
12.3XB	脆弱性なし
12.3XC	脆弱性なし
12.3XD	脆弱性なし
12.3XE	脆弱性なし
12.3XF	脆弱性なし
12.3XG	脆弱性なし
12.3XH	Vulnerable
12.3XI	脆弱性なし
12.3XJ	脆弱性なし
12.3XK	脆弱性なし

12.3XQ	Vulnerable
12.3XR	Vulnerable
12.3XS	脆弱性なし
12.3XU	Vulnerable
12.3XW	SIPポートは12.3(14)YX2以降ではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が存在します
12.3XX	SIPポートは12.3(8)XX2以降ではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が存在します
12.3XY	Vulnerable
12.3YA	脆弱性なし
12.3YD	脆弱性なし
12.3YF	SIPポートは12.3(14)YX2以降ではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が存在します
12.3YG	SIPポートは12.3(8)YG5以降ではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が存在します
12.3YH	脆弱性なし

12.3YI	脆弱性なし	
12.3YJ	脆弱性なし	
12.3YK	Vulnerable	
12.3YM	SIPポートは12.3(14)YM8以降ではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が存在します	
12.3YQ	Vulnerable	
12.3YS	脆弱性なし	
12.3YT	Vulnerable	
12.3YU	Vulnerable	
12.3YX	SIPポートは12.3(14)YX2以降ではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が存在します	
12.3YZ	Vulnerable	
該当する 12.4 ベースのリリース	リビルド	メンテナンス
12.4	SIPポートは、次に示すリリースではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が残っています	

	12.4(3d)	
	12.4(5b)	
	12.4(7a)	12.4(8)
12.4MR	SIPポートは12.4(6)MR以降ではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が存在します	
12.4SW	脆弱性あり。SIPポートがデフォルトで閉じられているすべての12.4SWリリースで回避策が利用可能	
12.4T	SIPポートは、次に示すリリースではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が残っています	
	12.4(2)T5	
	12.4(4)T3	
	12.4(6)T1	12.4(9)T
12.4XA	Vulnerable	
12.4XB	SIPポートは12.4(4)XB2以降ではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が存在します	
12.4XC	SIPポートは、2007年2月12日に入手可能な12.4(4)XC6*ではデフォルトで閉じられ	

	ていますが、SIPを実行しているルータには脆弱性が存在します
12.4XD	SIPポートは12.4(4)XD2以降ではデフォルトで閉じられていますが、SIPを実行しているルータには脆弱性が存在します
12.4XE	脆弱性あり。SIPポートがデフォルトで閉じられているすべての12.4XEリリースで回避策が利用可能
12.4XG	脆弱性なし
12.4XJ	脆弱性あり。SIPポートがデフォルトで閉じられているすべての12.4XJリリースで回避策が利用可能
12.4XP	脆弱性あり。SIPポートがデフォルトで閉じられているすべての12.4XPリリースで回避策が利用可能
12.4XT	脆弱性あり。SIPポートがデフォルトで閉じられているすべての12.4XTリリースで回避策が利用可能

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この問題は、お客様からシスコに最初に報告されたものです。この問題が意図的に悪用された例は報告されていません。ただし、この脆弱性を偶然に誘発したものと思われるデータ ストリームは観察されています。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070131-sip

改訂履歴

Revision 2.1	2007年2月10日	アドバイザリテーブルの形式と表現が変更されました。
Revision 2.0	2007年2月9日	ポート5060が開いているすべての製品に脆弱性が存在することを反映するようにドキュメントを更新。 「脆弱性のある製品」をボイスゲートウェイ、SBC、およびCAT6000-CMMで更新。 ソフトウェアテーブルを更新し、12.3(4)XH、12.3(4)XQ、12.3(7)XR、12.3(7)XS、12.3(8)JA、12.3(8)XU、12.3(8)XW、12.3(8)XX、12.3(8)XY、12.3(8)YA、12.3(8)YH、12.3 (8)YIおよび12.3(8)ZA。
リビジョン 1.1	2007年1月31日	アドバイザリに記載されているすべてのバグに対する共通脆弱性評価システム(CVSS)スコアを追加。 脆弱性の根本原因を追跡するCisco Bug IDとしてCSCsh58082(登録ユーザ専用)を追加。 文言の軽微な変更
リビジョン 1.0	2007年1月31日	初回公開リリース

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。