SIP パケットは SIP のためのサポートの IOSデバイスをリロードします

Low

アドバイザリーID : cisco-sa-20070131-sip

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 : Yes

Cisco バグ ID : CSCsb25337 , CSCsh58082

CVE-2007-0648

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

セッション開始プロトコル（SIP）をサポートするインターネットワークオペレーティングシステム（IOS）の影響を受けたバージョンを実行する Ciscoデバイスは特定の一続きのパケットをデバイスのリロードに導くかもしれない脆弱性からポート 5060 に受け取るとき向かう影響を受けます。 SIP のために設定されないデバイスの TCP 5060 および UDP ポート 5060 にトラフィックを可能にするこの問題は関連不具合によって混合します。

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。

回避策は SIP を必要としないデバイスのこの問題の効果を軽減するためにあります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070131-sip で掲示されます。

該当製品

修正済みソフトウェア

IOS およびサポート SIP 処理の脆弱なバージョンを実行するどの Ciscoデバイスでも脆弱であ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)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 が前に含まれています。 SIP Public Switched Telephone Network（PSTN）ゲートウェイで

設定されるルータは SIP セッション ボーダー コントローラ (SBCs) および CAT6000-CMM カードで設定されるルータであるように、脆弱です。

デバイスに有効に なる SIP があったかどうか確認するためにコマンド **show ip sockets** および **show tcp 要約をすべて**入力して下さい。 ルータ実行中のコードの例は修正と有効に なる回避策なしに下記にあります。 この例のルータは脆弱 な イメージ c7200-p-mz.124-3.bin を実行しています:

```
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。

```
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 処理をサポートしないデバイスはこの問題から影響を受けません。 これは含んでいますが、6500、7600、10000 シリーズおよび 12000 シリーズに制限されません。 ポート TCP 5060 および UDP 5060 がコマンド **show tcp 要約**が付いているデバイス**すべて**および **show ip sockets** で開いていないことをデバイスがこの問題に脆弱ではないことを確認するために、確認して下さい。 この問題に**脆弱**の修正された イメージ c7200-js-mz.124-5b.bin を実行するルータの例は下記にあります。

```
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 が付いている行は示されていないし、UDP SIP は有効に なりません。 この例では、UDP ポート 67 はこの脆弱性と関連していない DHCP によって使用されます。

改訂履歴

Revision 2.1	2007-February-10	諮問表の変更されたフォーマッティングおよび言葉遣い。
Revision	2007-February	開港 5060 が付いているすべての製品が脆弱であることを反映する更新されたドキュメント。 音声ゲートウェイが付いている更新済脆弱性

2.0	-9	が存在する製品、SBCs および CAT6000-CMM。 ソフトウェア テーブルを 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 の脆弱性を反映するためにアップデートしました。
リビジョン 1.1	2007-January-31	アドバイザリで述べられるすべてのバグのために記録する追加されたよくある脆弱性採点法（CVSS）。 脆弱性の根本的な原因をトラッキングする Cisco バグ ID として追加された CSCsh58082（登録ユーザのみ）。 マイナー な言葉遣い変更。
リビジョン 1.0	2007-January-31	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。