TCPループバックDoS攻撃(land.c)とシスコデバイス

アドバイザリーID : cisco-sa-19971121-land
初公開日 : 1997-11-21 22:00
バージョン 6.0 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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

誰かが、さまざまなTCP実装に対するサービス拒否攻撃を開始するために使用できる、land.cと呼ばれるプログラムをリリースしました。プログラムはTCP SYNパケット（接続開始）を送信し、ターゲットホストのアドレスを送信元と宛先の両方として指定し、ターゲットホスト上の同じポートを送信元と宛先の両方として使用します。

- 従来のCisco IOSソフトウェア（製品番号が1000より大きいCiscoルータ、CGS/MGS/AGS+上、CS-500上、およびバリアント形式でLightstream 1010 ATMスイッチ上で使用）は、ソフトウェアバージョンによっては、この攻撃に対して脆弱であることが確認されています。該当するバージョンについては、このドキュメントの「ソフトウェアバージョンと修正」セクションを参照してください。
- Cisco IOS/700ソフトウェア（Cisco 7xxルータで使用）にも脆弱性があることが確認されています。
- Catalyst 5xxxおよび29xx LANスイッチには、この攻撃に対する脆弱性があります。シスコの初期のラボテストで障害が再現されなかった原因は、攻撃プログラムの実行に使用されているマシンのカーネルにエラーが発生したことにあります。他のCatalystスイッチはCatalyst 5xxxまたは29xxとTCPコードを共有せず、テストで脆弱性を示すこともありません。
- Cisco BPXおよびIGX WANスイッチには、特定の状況において脆弱性が存在します。これらのスイッチは、中継データストリームからではなく、管理ポートを介してだけ攻撃される可能性があります。
- AXISシェルフはこの攻撃の影響を受けます。AXISシェルフは、その管理ポートを介してのみ攻撃できます。
- PIX Firewallはテスト済みで、この脆弱性には該当しません。
- Centriファイアウォールはテスト済みであり、この脆弱性には該当しません。

このアドバイザリは、

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19971121-landで公開されます。

該当製品

脆弱性のある製品

信頼できないホストからTCP経由で到達できるすべてのCisco IOS/700ソフトウェアシステムが影響を受けます。脆弱性のあるバージョンを実行し、信頼できないホストからTCP経由で到達できる従来のCisco IOSソフトウェアシステムが影響を受けます。信頼できないホストからTCP経由で到達できるすべてのCisco Catalyst 5xxxおよび29xxスイッチが影響を受けます。IGXおよびBPX WANスイッチとAXISシェルフは影響を受けますが、それらの管理ポートが悪意のあるパケットにさらされている場合に限られます。

いずれの場合も、攻撃によって到達可能なTCPポートは、実際にサービスが提供されているポート（ほとんどのシステムではTelnetポートなど）である必要があります。この攻撃では、ターゲット自身のアドレスをスプーフィングする必要があるため、効果的なアンチスプーフィングファイアウォールの背後にあるシステムは安全です。

脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

詳細

このセクションでは、これらの脆弱性に関する詳細情報を提供します。

Cisco IOS Software旧製品詳細

従来のCisco IOSソフトウェアバージョンは、land.c攻撃に対する脆弱性が異なります。リリースは、脆弱性が非常に高いクラス、中程度に脆弱性が高いクラス、および大部分が脆弱性を無効にするクラスに分類されます。新しいリリースは、古いリリースよりも脆弱性が低くなります。

Cisco IOS/700ソフトウェア

評価されたすべてのCisco IOS/700ソフトウェアバージョンはこの攻撃に対して脆弱です。この攻撃を受けたCisco IOS/700システムはハングするため、物理的にリセットする必要があります。

Cisco Catalyst 5xxxおよび29xx LANスイッチ

Cisco Catalyst 5xxxおよびCatalyst 29xx LANスイッチには、攻撃に対する脆弱性が存在します。両方のスイッチタイプが攻撃されるとクラッシュする。クラッシュの前にシステムハングが数秒程度かかる場合がありますが、システムが無期限にハングするようなことは確認されていません。この問題にはバグID CSCdj62723が割り当てられています。

他のCatalyst LANスイッチはテスト済みであり、攻撃に対する脆弱性は示されていません。該当するのは、5xxxシリーズと29xxシリーズだけです。

回避策

このセクションでは、これらの脆弱性の回避策について説明します。

Cisco IOS ソフトウェア

従来のCisco IOSソフトウェアユーザは、インターフェイスで入力アクセスリストを使用して、攻撃パケットがTCPスタックに入り込むのを防ぐことができます。入力アクセスリストは、9.21以降のすべてのCisco IOSソフトウェアバージョンで使用できます。入力アクセスリストを使用すると攻撃を完全に防止できますが、負荷の高いハイエンドルータでは許容できないパフォーマンスへの影響が発生する可能性があります。トラフィックは引き続きファーストスイッチングされますが、入力アクセスリストを使用して、より高速なスイッチングモードをディセーブルにできます。負荷の高いルータにこの回避策を導入する場合は注意してください。

既存の入力アクセスリストがない場合は、新しいIP拡張アクセスリストを作成します。100 ~ 199の間で現在使用されていない番号を使用します。アクセスリストには、システムで設定されている各IPアドレスのエントリが含まれている必要があります。各アドレスからそれ自体へのパケットを拒否します。例：

```
access-list 101 deny tcp 1.2.3.4 0.0.0.0 1.2.3.4 0.0.0.0
    access-list 101 deny tcp 5.6.7.8 0.0.0.0 5.6.7.8 0.0.0.0
    access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

既存のアクセスリストがある場合は、新しいエントリを適切な方法で（通常はリストの先頭に）マージする必要があります。

作成されたアクセスリストは、すべてのインターフェイスで着信に適用する必要があります。そのため、ルータの総設定のフラグメントは次のようになります。

```
interface ethernet 0
    ip address 1.2.3.4 255.255.255.0
    ip access-group 101 in
    !
    interface ethernet 1
    ip address 5.6.7.8
    ip access-group 101 in
    !
    access-list 101 deny tcp 1.2.3.4 0.0.0.0 1.2.3.4 0.0.0.0
    access-list 101 deny tcp 5.6.7.8 0.0.0.0 5.6.7.8 0.0.0.0
    access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

必要に応じて、この回避策をインストールしてアンチスプーフィングフィルタを確認することにより提供される機会を利用することを推奨します。

Cisco IOS/700ソフトウェア

次の設定コマンドを、潜在的に悪意のあるネットワークに接続されたときにアクティブになる可能性のあるプロファイルに追加します。

```
set ip filter tcp in source <7xx IP address> destination <7xx IP address> block
```

これにより、7xxシステムが完全に保護されます。このコマンドで許容できないパフォーマンスやその他の影響が生じる7xx設定は、実際に存在する場合は非常にまれであると考えられます。

Catalyst 5xxxおよび29xx LANスイッチ

この攻撃は、CatalystスイッチにIPアドレスを割り当てないことで完全に回避できます。ただし、これは、すべてのリモート管理を無効にする効果があります。ネットワーク内の場所によっては、ルータアクセスリストまたは専用ファイアウォールでスイッチを保護できる場合があります。個々のスイッチを個別に保護するための適切なCiscoルータアクセスリストエントリの例を次に示します。

```
access-list 101 deny ip <switch-address> 0.0.0.0 <switch-address> 0.0.0.0
```

この1つのエントリは完全なアクセスリストではないため、目的のトラフィックを許可する他のエントリと組み合わせない限り使用しないでください。他にも、より一般的なフィルタが可能です。

他のシステムを保護するCisco製品の使用

この攻撃は、汎用トンネルがファイアウォールを介して有効になっていない限り、専用ファイアウォール製品であるPIXおよびCentriファイアウォールの背後にあるシステムに対して使用できるとは考えられません。このような設定は推奨されません。

境界ルータで適切に設計されたアンチスプーフィングアクセスリストを使用すると、インターネットからプライベートネットワークに攻撃が侵入するのを防ぐことができます。アクセスリストを使用して、IP送信元アドレスが内部ネットワーク上にあるが、外部インターネットに接続されたインターフェイスから着信するパケットをフィルタリングします。このようなフィルタが強く推奨されるのは、この攻撃だけでなく、さまざまなネットワークデバイスに影響を与える他の既知の攻撃や、新しいIPスプーフィング攻撃が常に表面化するためです。可能な限り、内部ネット

ワークの一部ではない送信元アドレスを使用して内部ネットワークからインターネットにパケットが送信されないようにアクセスリストを設定することも望まれます。これは、ネットワークがサービス拒否攻撃のスタートパッドとして使用されないようにするのに役立ちます。

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

該当するバージョン

Cisco IOSソフトウェアがこの攻撃に対して脆弱になる原因となる2つのバグがあります。フィールドには両方のバグの修正が存在します。Bug ID CSCdi71085により、システムは攻撃に対して非常に脆弱になります。バグID CSCdi87533により、システムは中程度の脆弱性を持つようになります。バグID CSCdj61324は新しく作成されたバグIDで、CSCdi87533の修正を組み込むためのタグとして使用されます。また、ハーフオープン接続を一時的に作成することさえ妨げる大幅な変更が行われます。CSCdj61324の修正は、まだリリースされたコードに組み込まれていませんが、CSCdi87533の修正が存在する場合は必要ありません。

Cisco IOSソフトウェアのバージョンは、CSCdi71085とCSCdj87533によって3つの脆弱性クラスに分類されます。Bug ID CSCdi71085の修正が取り込まれていないバージョンは脆弱性が非常に高く、無期限でハングする可能性があります。攻撃を受けると、ハードウェアのリセットが必要になります。これには、リリース10.3より前のすべてのリリースと、初期の10.3、11.0、11.1、および11.2バージョンが含まれます。CSCdi71085は、次の表に示す10.3、11.0、および11.1リリースだけでなく、11.2(2)、11.2(2)P、および11.2(2)Fでも修正されています。

CSCdi71085が修正されていても、CSCdi87533が存在するバージョンは、攻撃に対して脆弱です。これらのバージョンは、攻撃パケットを受信した後、約30秒間は新しいTCP接続を受け入れませんが、完全にはハングせず、中断することなくパケットを転送し続け、長期的な影響なく回復します。これまでCSCdi87533は11.2ベースのリリースでのみ修正されており、修正は11.2(3.4)、11.2(3.4)F、および11.2(3.4)Pに組み込まれています。

CSCdi71085とCSCdi87533の両方が修正されたバージョンは、この攻撃に対して脆弱です。これらのバージョンは、攻撃パケットを受信するとハーフオープンTCP接続を作成しますが、正当なTCP接続を受け入れ続け、ハーフオープン接続を約30秒以内に削除します。このようなハーフオープン接続がライフタイムの間にパフォーマンスに与える影響は無視できるものと考えられます

。

CSCdj61324が修正された将来のバージョンでは、攻撃に対する脆弱性が存在し、攻撃パケットに対するハーフオープン接続は作成されません。シスコでは、CSCdj61324修正とCSCdj87533修正のセキュリティ上の利点は無視できるものと考えています。CSCdj61324は、今後の11.2以外のリリースで修正を統合する際に使用されるプレースホルダとなります。

システムに対する敵対的な攻撃の可能性があると考えられ、上記の設定回避策を使用して自身を保護できない場合、この攻撃でのCSCdi71085の影響は非常に大きいため、ソフトウェアをCSCdi71085の修正を含むバージョンに更新することを強くお勧めします。CSCdi71085に対する修正は、10.3、11.0、11.1、および11.2に基づくリリースで利用可能であり、かなり前からフィールドに存在していました。11.2ベースのリリースのユーザは、11.2(4)以降のバージョンをインストールして、CSCdi87533の修正も取得する必要があります。

このドキュメントの作成時点では、次のリリースが推奨されます。

基本リリース	最初にリリースされたバージョンとすべての既存の修正(CSCdi87533の修正*=含む)	ほとんどのインストールに推奨
10.3	10.3(16)	10.3(19a)
11.0	11.0(12)、11.0(12a)BT	11.0(17)、 11.0(17)BT
11.1	11.1(7)、11.1(7)AA、 11.1(7)CA、11.1(9)IA	11.1(15)、 11.1(15)AA、 11.1(15)CA、 11.1(15)IA
11.2	11.2(4)*、11.2(4)F*、11.2	11.2(10)、 11.2(9)P、 11.2(4)F1
10.3より前	エンジニアリング終了	10.3(19a)

他のソフトウェアアップデートと同様に、インストールする前に、システム設定が新しいソフトウェアでサポートされていることを確認する必要があります。新しいソフトウェアをサポートするのに十分なメモリがシステムにあることを確認することが特に重要です。アップデート計画の支援は、シスコのWorldwide Webサイトhttp://www.cisco.com/から入手できます。

計画済み修正

シスコでは、11.2以外のリリースに対してCSCdj61324(CSCdi87533に相当)の修正をリリースする予定です。CSCdj61324/CSCdi87533の影響は中程度であり、設定に関する回避策が存在するため、これらの修正に対して特別なソフトウェアリリースを作成する予定はありません。修正は、11.0および11.1ソフトウェアの定期的にスケジュールされたメンテナンスリリースに表示されます。この問題の回避策の詳細は、このドキュメントの「回避策」セクションを参照してください。

リリース10.3はエンジニアリングの終わりであり、修正されません。10.3以前のコードを実行する必要があり、下記の回避策をインストールできず、攻撃を受ける可能性があると思われるお客様は、Cisco TACにお問い合せください。

11.0と11.1の修正済みコードはすでに作成され、単体テストが行われており、現在は将来のメンテナンスリリースでの統合が予定されています。これらの修正は優先項目として扱われます。

Cisco IOS/700ソフトウェア

シスコでは、IOS/700のソフトウェア修正をリリースする予定です。修正コードはすでに作成されており、統合とリリースのテストが行われています。攻撃に対する完全な保護を提供する影響の少ない設定回避策があるため、シスコはこのソフトウェア修正プログラムのリリースを迅速に行う予定はありません。この修正は、定期的にスケジュールされたIOS/700メンテナンスリリースに表示されます。

Catalyst 5xxxおよび29xx LANスイッチ

Catalyst 5xxxおよび29xxスイッチソフトウェア用のソフトウェア修正が開発されています。これらのスイッチに対するland.c攻撃の影響は甚大であり、使用可能な設定上の回避策は多くのお客様にとって実用的ではないため、シスコではこれらの修正を組み込んだ暫定ソフトウェアビルドを作成しています。2.1(1102)と2.4(401)の2つの暫定バージョンがあります。

暫定バージョンは、通常のソフトウェアリリースよりもテストの対象が少なく、暫定バージョンに関するシスコのサポートリソースは、通常のリリースに関するサポートリソースよりも制限されています。お客様がこれらのリリースをインストールするのは、ネットワークが破壊的な攻撃の真のリスクにさらされていると考えられる場合だけにしてください。暫定ソフトウェアを入手するには、Cisco TAC(+1 800 553 24HR)にお問い合わせください。

この修正は、Catalyst 5xxxおよび29xxソフトウェアの2.1および2.4の次回の定期メンテナンスリリースに組み込まれます。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

シスコでは、この脆弱性に関して複数のレポートを用意しています。

ほとんどの不正利用は、一度に1つのパケットを送信する元のプログラムを使用しているようです。同様のプログラムlatierra.cがリリースされました。このプログラムはフラッディングを実行し、ポートとアドレスの範囲をスキャンします。フラッディング攻撃を受けると考えられます。

この問題は、さまざまなインターネットフォーラムで広く議論されています。エクスプロイトコードは広く一般に公開されています。

シスコでは、11月21日（金）の朝にこの問題について最初に聞きました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19971121-land

改訂履歴

リビジョン 6.0	1997年12月10日	Catalyst 5000は情報を修正します。その他の修正に関する詳細情報。一般的な再フォーマット
リビジョン 5.0	1997年11月28日	編集と入力エラー訂正
リビジョン 4.0	1997年11月28日	Catalyst 5000 は脆弱性が存在し、2900も脆弱性の影響を受けます。社内での問題の再現に失敗した原因は、テスト設定のエラーです。他のCatalystスイッチも同じ設定を使用してテストされているため、脆弱性が存在する可能性があります。

リビジョン 3.0	1997年11月26日	Catalyst 5000が脆弱であるという主張を撤回します。IGXおよびBPX WANスイッチとAXISシェルフに関する情報を追加します。
Revision 2.0	1997年11月22日	脆弱性の高いCisco IOSバージョンに関する情報を追加します。 該当するバージョン番号に関する詳細情報を追加します。 特定のバグIDを追加します。 アップグレードの推奨事項を追加します。 Catalyst LANスイッチに関する最初の情報を追加します。 一般的な編集と再フォーマット
リビジョン 1.0	1997年11月21日	初期リビジョン

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。