UDP診断ポートのサービス拒否攻撃からの保護

内容

概要

ネットワークデバイスを対象とするISPにサービス拒否攻撃が発生する可能性があります。

- **ユーザデータグラムプロトコル(UDP)診断ポート攻撃**：送信者は、ルータ上で大量のUDP診断サービス要求を送信します。これにより、すべてのCPUリソースが偽の要求を処理するために消費されます。

このドキュメントでは、潜在的なUDP診断ポート攻撃の発生方法について説明し、それを防御するためにCisco IOS®ソフトウェアで使用する方法を提案します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。このドキュメントで参照されているコマンドの一部は、Cisco IOSソフトウェアリリース10.2(9)、10.3(7)、および11.0(2)、およびそれ以降のすべてのリリースでのみ使用できます。これらのコマンドは、Cisco IOSソフトウェアリリース12.0以降ではデフォルトです。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

問題の説明

UDP 診断ポート攻撃

デフォルトでは、Ciscoルータでは、特定のUDPおよびTCPサービスに対して一連の診断ポートが有効になっています。これらのサービスには、echo、chargen、およびdiscardがあります。ホストがこれらのポートに接続すると、これらの要求を処理するために少量のCPU容量が消費されます。

1台の攻撃デバイスがランダムな偽の送信元IPアドレスを持つ大量の要求を送信すると、Ciscoルータが過負荷になり、速度が低下したり、障害が発生したりする可能性があります。

この問題は、外面上はプロセス テーブルが満杯になったことを示すエラー メッセージ（%SYS-3 NOPROC）や CPU 使用率の大幅な上昇といった症状として現れます。execコマンド**show process**は、「UDP Echo」などの同じ名前の多数のプロセスを表示します。

ネットワークデバイスへの直接攻撃から防御

UDP診断ポートの無効化

UDPおよびTCP診断サービスを備えたネットワークデバイスは、ファイアウォールで保護するか、サービスを無効にする必要があります。Cisco ルータでサービスを無効にするには、次のグローバル設定コマンドを使用します。

```
no service udp-small-servers
no service tcp-small-servers
```

これらのコマンドの詳細については、「付録」を参照してください。このコマンドは Cisco IOS ソフトウェア リリース 10.2（9）、10.3（7）、および 11.0（2）で導入され、それ以降のすべてのリリースで使用できます。これらのコマンドは、Cisco IOSソフトウェアリリース12.0以降ではデフォルトです。

ネットワークが無意識のうちに攻撃をホストするのを防ぐ

サービス拒否攻撃の基本的なメカニズムはランダムな IP アドレスを送信元とするトラフィックを生成することであるため、インターネットに送信されるトラフィックをフィルタリングすることをお勧めします。基本的に、「無効な送信元 IP アドレスを持つパケットがあればインターネットに入る前に廃棄する」と考えてください。これは、ネットワークに対するサービス拒否攻撃を防止するものではありません。ただし、攻撃を受けた側が攻撃者の送信元として自分の場所を除外するのに役立ちます。また、お客様のネットワークがこの種の攻撃に利用される事態も回避できます。

無効なIPアドレスの送信の防止

お客様のネットワークをインターネットに接続するルータ上でパケットをフィルタリングすれば、有効な送信元 IP アドレスを持つパケットだけをお客様のネットワークからインターネットに送信できます。

たとえば、ネットワークがネットワーク172.16.0.0で構成されていて、ルータがFDDI0/1インターフェイスを使用してISPに接続している場合、次のようなアクセスリストを適用できます。

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log [1]

interface Fddi 0/1
ip access-group 111 out
```

[1]アクセスリストの最後の行は、無効な送信元アドレスを持つトラフィックがインターネットに着信しているかどうかを判別します。これは、考えられる攻撃の原因を特定するのに役立ちます。

無効なIPアドレスの受信の防止

末端のネットワークにサービスを提供している ISP では、クライアントから到達する着信パケットを検証することをお勧めします。これを行うには、境界ルータ上で着信パケットのフィルタリングを行います。

たとえば、クライアントがこれらのネットワーク番号を「FDDI 1/0」という名前のFDDIインターフェイスを介してルータに接続している場合、このアクセスリストを作成できます。

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface Fddi 1/0
ip access-group 111 in
```

注：アクセスリストの最後の行は、無効な送信元アドレスを持つトラフィックがインターネットに入っているかどうかを判別します。これは、攻撃の可能性のある原因を特定するのに役立ちます。

付録：スモール サーバに関する説明

スモールサーバは、診断に役立つルータで実行されるサーバ（UNIX用語ではデーモン）です。したがって、デフォルトで動作しています。

TCP および UDP のスモール サーバに対するコマンドは次のとおりです。

- service tcp-small-servers
- service udp-small-servers

ルータに非ルーティングサービスを提供しない場合は、それらをオフにします(前のコマンドのno形式を使用)。

TCP スモール サーバには次の機能があります。

- **Echo**：入力した内容をエコーバックします。確認するには、telnet x.x.x.x echo とコマンドを入力してください。
- **Chargen**:ASCIIデータのストリームを生成します。確認するには、telnet x.x.x.x chargen とコマンドを入力してください。
- **Discard**：入力した内容を破棄します。確認するには、telnet x.x.x.x discard とコマンドを入力してください。
- **Daytime**：システムの日付と時刻が正しければ返されます。NTPを実行している場合、またはEXECレベルから手動で日付と時刻を設定している場合は正しいです。確認するには、telnet x.x.x.x daytime とコマンドを入力してください。

UDP スモール サーバには次の機能があります。

- **Echo**：送信したデータグラムのペイロードをエコーします。
- **Discard**：送信したデータグラムをサイレントピッチで送信します。
- **Chargen**：送信するデータグラムをピッチし、CR+LFで終了する72文字のASCII文字列で応答します。

注：ほぼすべてのUNIXボックスは、上記のスモールサーバをサポートしています。ルータは、fingerサービスとasync line bootpサービスも提供します。これらは、グローバルコンフィギュレーションコマンド**no service finger**と**no ip bootp server**を**それぞれ使**用して**個別にオフに**できます。

関連情報

- Cisco IOS ソフトウェア
- テクニカルサポート - Cisco Systems