目次

概要

その ISP に潜在的なDoS攻撃がターゲット ネットワークデバイスあります。

- **User Datagram Protocol （ UDP; ユーザ データグラム プロトコル ） 診断ポート攻撃:** 送信側はルータの UDP 診断サービスのための要求の音量を送信します。 これはすべての CPU リソースを偽りの要求を保守するために消費します。

可能性 UDP 診断ポート攻撃がどのように発生する記述され、Cisco IOS® ソフトウェアと使用するようにメソッドを提案しますかこの資料にそれに対して守るために。

前提条件

要件

このドキュメントに関する固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。 いくつかのこの資料で参照されるコマンドは Cisco IOS ソフトウェア リリースの利用可能 な開始だけ 10.2(9)、10.3(7)、および 11.0(2)、およびすべての後続のリリースです。 これらのコマンドは Cisco IOS ソフトウェア release 12.0 と それ以降のデフォルトです。

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、Ciscoルータはある特定の UDP および TCP サービスのために有効に なる一連の診断 ポートを備えています。 これらのサービスはエコー、chargen および廃棄が含まれています。 ホストがこれらのポートに接続するときこれらの要求を保守するために、わずか CPU キャパシティは消費されます。

単一攻撃デバイスが異なる、ランダムの、偽りのソース IP アドレスの要求の大きい弾幕を送信すれば、Ciscoルータが圧倒されるようになり、減速するか、または壊れることは可能性のあるです。

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 は表示します「UDP エコーのような同じ名前の多くのプロセスを」。

ネットワークデバイスに不正侵入に対して直接守って下さい

UDP 診断 ポートを無効にして下さい

ファイアウォールによって保護される UDP および TCP 診断サービスが必要あるまたはサービスがありますディセーブルにされるどのネットワークデバイスでも。 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-serversno 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 release 12.0 と それ以降のデフォルトです。

ネットワークが無意識のうちに攻撃をホストすることを防いで下さい

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のサービス拒否攻撃を防ぎません。 ただし、それは攻撃されたパーティが攻撃者のソースとして宛先住所を除外するのを助けます。 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 アドレスの送信を防いで下さい

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 で構成されていれば、およびルータ FDDI0/1 イ

ンターフェイスを使用して ISP に、このようなアクセス リストを追加できます接続します:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 anyaccess-list 111 deny ip any any log
¹interface Fddi 0/1ip access-group 111 out
```

¹はアクセス リストの最後の行インターネットを入力する無効な送信元アドレスとのトラフィックがあったかどうか確認します。 これは可能性のある不正侵入のソースを見つけるのを助けます。

無効 な IP アドレスの受信を防いで下さい

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、クライアントに「FDDI 1/0" と指名される FDDI インターフェイスを通してルータに接続されるこれらのネットワーク番号があればこのアクセス リストを作成できます。

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0access-list 111 permit ip
192.168.0.0 0.0.15.255 anyaccess-list 111 permit ip 172.18.0.0 0.0.255.255 anyaccess-list 111
deny ip any any loginterface Fddi 1/0ip access-group 111 in
```

注アクセス リストの最後の行はインターネットを入力する無効な送信元アドレスとのトラフィックがあったかどうか確認します。 これは可能性のある 攻撃のソースを見つけるのを助けます。

付録： スモール サーバに関する説明

小さいサーバは診断に役立つサーバ (UNIX用語のデーモン、) ルータのその実行です。 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 サービスを提供してほしくない場合それらを消して下さい (前のコマンドの **no 形式**を使用して) 。

TCP スモール サーバには次の機能があります。

- **エコー**か。エコーは入力するものは何でも支持します。 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** か。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。
- **廃棄して下さい**か。入力されたものを廃棄します。 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。
- **昼間**か。正しかったら戻りシステムの日付および時間。 それは NTP を実行するか、または exec レベルからの日時を手動で 設定 したら正しいです。 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。

- **エコー**か。送信したデータグラムのペイロードをエコーします。
- **廃棄して下さい**か。送信したダイアグラムを調整し、応答しない。

- **Chargen** か。送信したダイアグラムを調整し、CR+LF で終了する 72 文字の ASCII 文字列で応答。x.x.x.x の部分は、任意のルータのアドレスで置き換えてください。

注ほとんどすべての UNIXボックスは以前にリストされている小さいサーバをサポートします。ルータはまたフィンガー サービスおよび非同期回線 BOOTPサービスを提供します。 これらは設定 グローバルコマンド **no service finger** および **no ip bootp server** と独自にそれぞれ消すことができます。

関連情報

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