Contenu

Introduction

Il y a une attaque de refus de service potentielle aux ISP des périphériques de ce réseau de cibles.

- **Attaque diagnostique de port de Protocole UDP (User Datagram Protocol) :** Un expéditeur transmet un volume de demandes des services diagnostiques d'UDP sur le routeur. Ceci cause toutes les ressources CPU d'être consommées pour entretenir les fausses demandes.

Ce document décrit comment l'attaque diagnostique de port d'UDP potentiel se produit et suggère les méthodes pour l'utiliser avec le logiciel de Cisco IOS® afin de défendre contre lui.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. Certaines des commandes visées à ce document sont seulement commencer disponible dans des versions du logiciel Cisco IOS 10.2(9), 10.3(7), et 11.0(2), et toutes les versions suivantes. Ces commandes sont le par défaut dans le Logiciel Cisco IOS version 12.0 et plus tard.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives

aux conseils techniques Cisco.

Description du problème

L'attaque diagnostique de port d'UDP

Par défaut, le routeur de Cisco a une gamme de ports diagnostiques activés pour des services de certain UDP et de TCP. Ces services incluent l'écho, le chargen, et l'écart. Quand un hôte se relie à ces ports, un peu de capacité CPU est consommée d'entretenir ces demandes.

Si un périphérique de attaque simple envoie un grand barrage des demandes avec différentes, aléatoires, fausses adresses IP de source, il est possible que le routeur de Cisco devienne accablé et ralentit ou échoue.

La manifestation externe du problème inclut un plein message d'erreur de table de processus (`%SYS-3 NOPROC`) ou très une utilisation du CPU élevé. **Le processus d'exposition de** commande EXEC affiche beaucoup de processus avec le même nom, tel que le « écho d'UDP. »

Défendez contre des attaques directement aux périphériques de réseau

Ports de diagnostic d'UDP de débronchement

N'importe quel périphérique de réseau qui a l'UDP et des services diagnostiques de TCP doit être protégé par un Pare-feu ou ont les services désactivés. Pour un routeur de Cisco, ceci peut faire à l'aide de ces commandes de configuration globale.

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

Voyez l'annexe pour plus d'informations sur ces commandes. Les commandes sont commencer disponible dans des versions du logiciel Cisco IOS 10.2(9), 10.3(7), et 11.0(2) et toutes les versions suivantes. Ces commandes sont le par défaut dans le Logiciel Cisco IOS version 12.0 et plus tard.

Empêchez le réseau d'accueillir inconsciemment une attaque

Puisqu'un mécanisme primaire des attaques par déni de service est la génération du trafic originaire des adresses IP aléatoires, Cisco recommande le trafic de filtrage destiné pour l'Internet. Le concept de base est de jeter des paquets avec des adresses IP de source non valide car ils entrent dans l'Internet. Ceci n'empêche pas l'attaque par déni de service sur votre réseau. Cependant, il aide les interlocuteurs attaqués à éliminer votre emplacement comme source de l'attaquant. En outre, il empêche l'utilisation de votre réseau pour cette classe des attaques.

Empêchez la transmission des adresses IP non valides

En filtrant des paquets sur vos Routeurs qui connectent votre réseau à l'Internet, vous pouvez permettre seulement à des paquets avec les adresses IP valides de source pour laisser votre réseau et pour l'entrer dans l'Internet.

Par exemple, si votre réseau se compose du réseau 172.16.0.0, et votre routeur se connecte à votre ISP utilisant une interface FDDI0/1, vous peut appliquer la liste d'accès comme ceci :

```
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
```

Le ¹ la dernière ligne de la liste d'accès détermine s'il y a n'importe quel trafic avec une adresse source incorrecte qui entre dans l'Internet. Ceci aide à identifier la source des attaques possibles.

Empêchez la réception des adresses IP non valides

Pour les ISP qui fournissent le service pour finir des réseaux, Cisco recommande fortement la validation des paquets entrant de vos clients. Ceci peut faire en employant des filtres de paquets entrant sur vos Routeurs de cadre.

Par exemple, si vos clients ont ces network number connectés à votre routeur par une interface FDDI nommée « FDDI 1/0", vous pouvez créer cette liste d'accès.

```
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
```

Remarque: La dernière ligne de la liste d'accès détermine s'il y a n'importe quel trafic avec une adresse source incorrecte qui entre dans l'Internet. Ceci aide à identifier la source d'attaque possible.

Annexe : Description de petits serveurs

Les petits serveurs sont les serveurs (démons, dans le langage UNIX) ce passage dans le routeur qui sont utiles pour des diagnostics. Par conséquent, ils sont allumés par défaut.

Les commandes pour les petits serveurs de TCP et UDP sont :

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

Si vous ne voulez pas que votre routeur ne fournisse aucun services de non-routage, arrêtez-les (utilisant le **forme no des** commandes précédentes).

Les petits serveurs de TCP sont :

- **Écho** ? Les échos soutiennent celui que vous tapiez. Tapez l'**écho du telnet x.x.x.x de** commande **pour voir**.
- **Chargen** ? Génère un flot des données ASCII. Tapez le **chargen du telnet x.x.x.x de** commande **pour voir**.
- **Jetez** ? Jette celui que vous tapiez. Tapez l'**écart du telnet x.x.x.x de** commande **pour voir**.
- **En journée** ? Retours date du système et temps, si correct. Il est correct si vous exécutez le NTP ou avez placé la date et l'heure manuellement du niveau d'exécutif. Tapez l'**en journée du telnet x.x.x.x de** commande **pour voir**.

Les petits serveurs d'UDP sont :

- **Écho** ? Fait écho la charge utile du datagramme que vous envoyez.
- **Jetez** ? Lance silencieusement le datagramme que vous envoyez.

- **Chargen** ? Lance le datagramme que vous envoyez et répond avec une chaîne des caractères 72 des caractères ASCII terminés avec un CR+LF.

Remarque: Presque toutes les copies d'Unix prennent en charge les petits serveurs précédemment répertoriés. Le routeur offre également le service de BOOTP de service et de ligne asynchrone de Finger. Ceux-ci peuvent être indépendamment arrêtés avec les commandes globales de configuration **aucun service finger** et **aucun ip bootp server**, respectivement.

Informations connexes

- Logiciel Cisco IOS
- Support technique - Cisco Systems