Protection contre les attaques par déni de service de port de diagnostic UDP

Contenu

Introduction

Il existe une attaque potentielle de déni de service sur les FAI qui cible les périphériques réseau.

- **Attaque de port de diagnostic UDP (User Datagram Protocol) :** Un expéditeur transmet un volume de demandes de services de diagnostic UDP sur le routeur. Cela entraîne la consommation de toutes les ressources du processeur pour le service des demandes bidon.

Ce document décrit comment se produit l'attaque potentielle de port de diagnostic UDP et suggère les méthodes à utiliser avec le logiciel Cisco IOS® afin de se défendre contre elle.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. Certaines des commandes mentionnées dans ce document ne sont disponibles qu'à partir des versions du logiciel Cisco IOS 10.2(9), 10.3(7) et 11.0(2), ainsi que de toutes les versions ultérieures. Ces

commandes sont les commandes par défaut du logiciel Cisco IOS Version 12.0 et ultérieure.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Description du problème

Attaque de port de diagnostic UDP

Par défaut, une série de ports de diagnostic est activée sur le routeur Cisco pour certains services UDP et TCP. Ces services incluent l'écho, la facturation et l'abandon. Lorsqu'un hôte se connecte à ces ports, une petite quantité de capacité de CPU est consommée pour traiter ces requêtes.

Si un seul périphérique d'attaque envoie un grand nombre de requêtes avec des adresses IP source différentes, aléatoires et fausses, il est possible que le routeur Cisco soit submergé et ralentit ou échoue.

La manifestation externe du problème inclut un message d'erreur complet de la table de processus (`%SYS-3 NOPROC`) ou une utilisation CPU très élevée. La commande exec **show process** montre un grand nombre de processus portant le même nom, comme « UDP Echo ».

Protégez vos périphériques réseau contre les attaques

Désactiver les ports de diagnostic UDP

Tout périphérique réseau disposant de services de diagnostic UDP et TCP doit être protégé par un pare-feu ou les services doivent être désactivés. Pour un routeur Cisco, vous pouvez effectuer cette opération à l'aide de ces commandes de configuration globale.

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

Reportez-vous à l'annexe pour plus d'informations sur ces commandes. Les commandes sont disponibles à partir des versions du logiciel Cisco IOS 10.2(9), 10.3(7) et 11.0(2) et de toutes les versions ultérieures. Ces commandes sont les commandes par défaut du logiciel Cisco IOS Version 12.0 et ultérieure.

Empêcher le réseau d'héberger involontairement une attaque

Étant donné que le principal mécanisme d'attaque par déni de service est la génération du trafic provenant d'adresses IP aléatoires, Cisco recommande de filtrer le trafic destiné à Internet. Le concept de base est de jeter les paquets avec des adresses IP source non valides lorsqu'ils pénètrent sur Internet. Cela n'empêche pas l'attaque par déni de service sur votre réseau. Cependant, cela aide les parties attaquées à exclure votre emplacement comme source de l'attaquant. En outre, il empêche l'utilisation de votre réseau pour cette classe d'attaques.

Empêcher la transmission d'adresses IP non valides

En filtrant les paquets sur vos routeurs qui connectent votre réseau à Internet, vous pouvez autoriser uniquement les paquets avec des adresses IP source valides à quitter votre réseau et à accéder à Internet.

Par exemple, si votre réseau se compose du réseau 172.16.0.0 et que votre routeur se connecte à votre FAI à l'aide d'une interface FDDI0/1, vous pouvez appliquer la liste d'accès comme suit :

```
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]La dernière ligne de la liste d'accès détermine s'il existe un trafic avec une adresse source non valide qui entre sur Internet. Cela permet de localiser la source des attaques possibles.

Empêcher la réception d'adresses IP non valides

Pour les FAI qui fournissent des services aux réseaux finaux, Cisco recommande vivement la validation des paquets entrants de vos clients. Pour ce faire, vous pouvez utiliser des filtres de paquets entrants sur vos routeurs périphériques.

Par exemple, si vos clients ont ces numéros de réseau connectés à votre routeur via 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 172.18.0.0

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
```

Remarque : La dernière ligne de la liste d'accès détermine s'il existe un trafic avec une adresse source non valide qui entre sur Internet. Cela permet de localiser la source de l'attaque possible.

Annexe : Description des petits serveurs

Les petits serveurs sont des serveurs (démons, dans le langage UNIX) qui s'exécutent dans le routeur et qui sont utiles pour les diagnostics. Par conséquent, ils sont activés par défaut.

Les commandes des petits serveurs TCP et UDP sont les suivantes :

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

Si vous ne voulez pas que votre routeur fournisse des services non liés au routage, désactivez-les (en utilisant la forme **no** des commandes précédentes).

Les petits serveurs TCP sont les suivants :

- **Echo** (Echo) : permet d'extraire tout ce que vous tapez. Entrez la commande **telnet x.x.x.x echo** pour afficher.
- **Chargen** : génère un flux de données ASCII. Entrez la commande **telnet x.x.x.x** pour afficher.
- **Discard** : jette tout ce que vous tapez. Entrez la commande **telnet x.x.x.x discard** pour afficher.
- **Jour** : renvoie la date et l'heure système, si elles sont correctes. Il est correct si vous exécutez NTP ou avez défini manuellement la date et l'heure à partir du niveau exec. Tapez la commande **telnet x.x.x.x day** pour afficher.

Les petits serveurs UDP sont les suivants :

- **Écho** : fait écho à la charge utile du datagramme que vous envoyez.
- **Discard** : affiche silencieusement le datagramme que vous envoyez.
- **Chargen** : affiche le datagramme que vous envoyez et répond avec une chaîne de 72 caractères ASCII terminée par un CR+LF.

Remarque : Presque toutes les boîtes UNIX prennent en charge les petits serveurs précédemment répertoriés. Le routeur offre également le service finger et le service de démarrage de ligne asynchrone. Ils peuvent être désactivés indépendamment avec les commandes globales de configuration **no service finger** et **no ip bootp server**, respectivement.

Informations connexes

- Logiciel Cisco IOS
- Support technique - Cisco Systems