Bescherm tegen UDP: diagnostische poortontkenning van serviceaanvallen

Inhoud

Inleiding

Er is een mogelijke ontkenning-van-service aanval bij ISP's die netwerkapparaten herstelt.

- **User Datagram Protocol (UDP) diagnostische poortaanval:** Een afzender geeft een volume van verzoeken voor UDP diagnostische diensten op de router over. Dit zorgt ervoor dat alle CPU-bronnen worden gebruikt om de nepverzoeken te bedienen.

Dit document beschrijft hoe de potentiële UDP diagnostische poortaanval optreedt en stelt de methoden voor om met Cisco IOS® software te gebruiken om zich ertegen te verdedigen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies. Sommige van de opdrachten die in dit document worden vermeld, zijn alleen beschikbaar vanaf Cisco IOS-softwarereleases 10.2(9), 10.3(7) en 11.0(2) en alle latere releases. Deze opdrachten zijn de

standaardinstelling in Cisco IOS-softwarerelease 12.0 en hoger.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Beschrijving van probleem

De UDP diagnostische poortadapter

Standaard heeft de Cisco-router een reeks diagnostische poorten die zijn ingeschakeld voor bepaalde UDP- en TCP-services. Tot de diensten behoren echo, chargen en teruggooi. Wanneer een host aan deze poorten bevestigt, wordt een kleine hoeveelheid CPU-capaciteit gebruikt voor de service van deze verzoeken.

Als één enkel aanvallend apparaat een grote reeks verzoeken met verschillende, willekeurige, nepbron IP adressen verstuurt, is het mogelijk dat de Cisco router overweldigd wordt en vertraagt of mislukt.

De externe manifestatie van het probleem omvat een volledig foutbericht van de procestabel (`%SYS-3 NOPROC`) of een zeer hoog CPU-gebruik. Het exec commando **show proces** toont veel processen met dezelfde naam, zoals "UDP Echo".

Verdedig tegen aanvallen direct op netwerkapparaten

UDP-diagnostische poorten uitschakelen

Elk netwerkapparaat dat UDP en TCP diagnostische services heeft moet beschermd worden door een firewall of de services uitgeschakeld hebben. Voor een router van Cisco, kan dit worden verwezenlijkt door deze mondiale configuratieopdrachten te gebruiken.

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

Zie het Bijlage voor meer informatie over deze opdrachten. De opdrachten zijn beschikbaar vanaf 10.2(9), 10.3(7) en 11.0(2) van Cisco IOS-softwarereleases en alle latere releases. Deze opdrachten zijn de standaardinstelling in Cisco IOS-softwarerelease 12.0 en hoger.

Beletten dat het netwerk op onbedoelde wijze een aanval organiseert

Aangezien een primair mechanisme van denial-of-service aanvallen de generatie van verkeer is die uit willekeurige IP-adressen is voortgebracht, adviseert Cisco het filteren van verkeer dat voor het internet is bestemd. Het basisconcept is om pakketten met ongeldige bron-IP adressen weg te gooien wanneer zij het internet betreden. Dit verhindert niet de ontkenning-van-service aanval op uw netwerk. Maar het helpt de aangevallen partijen om je locatie als bron van de aanvaller uit te

sluiten. Bovendien voorkomt het het gebruik van uw netwerk voor deze klasse van aanvallen.

Beletten dat ongeldige IP-adressen worden verzonden

Door pakketten te filteren op uw routers die uw netwerk met het internet verbinden, kunt u alleen pakketten met geldige bron-IP-adressen toestaan om uw netwerk te verlaten en op het internet te komen.

Als uw netwerk bijvoorbeeld uit netwerk 172.16.0.0 bestaat en uw router met uw ISP verbindt met behulp van een FDDI0/1 interface, kunt u de toegangslijst als volgt toepassen:

```
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]De laatste regel van de toegangslijst bepaalt of er verkeer is met een ongeldig bronadres dat het internet binnenkomt. Dit helpt om de bron van de mogelijke aanvallen te vinden.

Beletten dat ongeldige IP-adressen worden ontvangen

Voor ISPs die de dienst om netwerken te beëindigen verlenen, adviseert Cisco zeer de validatie van inkomende pakketten van uw cliënten. Dit kan worden bereikt door het gebruik van inkomende pakketfilters in uw grensrouters.

Bijvoorbeeld, als uw cliënten deze netwerknummers hebben die met uw router door een interface FDDI genaamd "FDDI 1/0" worden verbonden, kunt u deze toegangslijst maken.

```
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
```

Opmerking: de laatste regel van de toegangslijst bepaalt of er verkeer is met een ongeldig bronadres dat op het internet komt. Dit helpt om de bron van de mogelijke aanval te vinden.

Bijlage: Beschrijving van kleine servers

De kleine servers zijn servers (daemons, in UNIX-apparatuur) die in de router worden uitgevoerd en die nuttig zijn voor diagnostiek. Daarom staan ze standaard aan.

De opdrachten voor de kleine TCP- en UDP-servers zijn:

- kleine serviceservers
- Service-UDP-kleine servers

Als u niet wilt dat uw router om het even welke niet-routeringsservices biedt, schakelt u deze uit (**zonder** de vorige opdrachten).

De TCP kleine servers zijn:

- **Echo**, kiest terug wat je typt. Typ de te zien opdracht **telnet x.x.x echo**.
- **Chargen** genereert een stroom ASCII gegevens. Typ de opdracht **telnet x.x.x.x** om te zien.
- **Gooi** weg wat je typt. Typ de **terugweg** van de opdrachttelefoon **x.x.x.x** om te zien.
- **Daytime**-Retourensysteemdatum en -tijd, indien correct. Het is correct als u NTP gebruikt of de datum en de tijd handmatig van het uitvoerniveau hebt ingesteld. Typ **het** opdrachttelnet **x.x.x dag** om te zien.

De kleine UDP-servers zijn:

- **Echo** — Hiermee selecteert u de lading van het datagram dat u stuurt.
- **Gooi** het datagram stilletjes weg.
- **Chargen**—Pitches het datagram dat u verstuurt en reageren met een 72-tekenstring van ASCII tekens die is afgesloten met een CR+LF.

Opmerking: Bijna alle UNIX-boxen ondersteunen de eerder genoemde kleine servers. De router biedt ook vingerservice en asynchrone lijnbootservice aan. Deze kunnen onafhankelijk worden uitgeschakeld met de configuratie global opdrachten **zonder servicetekens** en zonder IP bootp server.

Gerelateerde informatie

- Cisco IOS-software
- Technische ondersteuning - Cisco-systemen