Contenido

Introducción

Hay un rechazo potencial de ataques de servicio en los ISP esos los dispositivos de red de las blancos.

- **Establecimiento de puerto de diagnóstico del User Datagram Protocol (UDP):** Un remitente transmite un volumen de pedidos los servicios de diagnóstico UDP en el router. Esto hace a todos los recursos de la CPU ser consumida para mantener las falsas peticiones.

Este documento describe cómo ocurre el establecimiento de puerto de diagnóstico del potencial UDP y sugiere los métodos para utilizar con el software de Cisco IOS® para defender contra él.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. Algunos de los comandos mencionados en este documento son solamente el comenzar disponible en los Cisco IOS Software Release 10.2(9), 10.3(7), y 11.0(2), y todas las versiones posteriores. Estos comandos son el valor por defecto en el Cisco IOS Software Release 12.0 y Posterior.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Descripción de problemas

Establecimiento del puerto de diagnóstico UDP

Por abandono, el router Cisco tiene una serie con certeza de servicios habilitados los puertos de diagnóstico UDP y TCP. Estos servicios incluyen la generación de eco, el chargen, y el descarte. Cuando consumen a los attaches de un host a estos puertos, un muy poco de capacidad de CPU para mantener estas peticiones.

Si un solo dispositivo que ataca envía una presa grande de las peticiones con diferente, al azar, los IP Addresses de la fuente falsa, es posible que el router Cisco se abruma y retrasa o falla.

La manifestación externa del problema comprende un mensaje de error completo de tabla de procesos (%SYS-3 NOPROC) o un uso de CPU muy alto. **El proceso del** exec command show muestra muchos procesos con el mismo nombre, tal como “generación de eco UDP.”

Defienda contra los ataques directamente a los dispositivos de red

Inhabilite los puertos de diagnóstico UDP

Cualquier dispositivo de red que tenga los servicios de diagnóstico UDP y TCP necesita ser protegido por un Firewall o tiene los servicios inhabilitados. En un router de Cisco esto puede lograrse mediante estos comandos de configuración global.

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

Para más información sobre estos comandos consulte el Apéndice . Los comandos están disponibles a partir de las versiones 10.2(9), 10.3(7) y 11.0(2) del software IOS de Cisco y todas las versiones subsiguientes. Estos comandos son el valor por defecto en el Cisco IOS Software Release 12.0 y Posterior.

Evite que la red reciba involuntariamente un ataque

Dado que un mecanismo primario de ataques de rechazo del servicio es la generación del tráfico originado en las direcciones IP aleatorias, Cisco recomienda el filtrado del tráfico destinado a Internet. El concepto básico es descartar paquetes con direcciones IP de origen no válidas a medida que ingresan a Internet. Esto no previene el establecimiento de rechazo del servicio en su red. Sin embargo, ayuda a los partidos atacados a eliminar su ubicación como la fuente del atacante. Además, impide el uso de la red para esta clase de ataques.

Prevenga la transmisión de IP Addresses no válidos

Al filtrar paquetes en los routers que conectan la red a Internet, puede permitir que únicamente los paquetes con direcciones IP de origen válidas abandonen la red y lleguen a Internet.

Por ejemplo, si su red consiste en la red 172.16.0.0, y su router conecta con su ISP usando una interfaz FDDI0/1, usted puede aplicar la lista de acceso como esto:

```
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
```

¹que la línea más reciente de la lista de acceso determina si hay algún tráfico con una dirección de origen no válida que ingrese el Internet. Esto ayuda a localizar la fuente de los ataques posibles.

Prevenga la recepción de las dirección IP no válidas

Para los ISP que proporcionan servicios a las redes extremas, Cisco recomienda la validación de los paquetes entrantes de sus clientes. Esto se logra usando filtros de paquete de entrada en los routers de borde.

Por ejemplo, si sus clientes tienen estos network number conectados con su router a través de una interfaz FDDI nombrada “FDDI el 1/0", usted puede crear esta lista de acceso.

```
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
```

Nota: La línea más reciente de la lista de acceso determina si hay algún tráfico con una dirección de origen no válida que ingrese el Internet. Esto ayuda a localizar la fuente del ataque posible.

Apéndice: Descripción de servidores pequeños

Los pequeños servidores son los servidores (daemones, en el término de Unix) ese funcionamiento en el router que son útiles para los diagnósticos. Por lo tanto, están en funcionamiento por defecto.

Los comandos para los servidores TCP y UDP pequeños son los siguientes:

- **mantenga los TCP-pequeño-servidores**
- **service udp-small-servers**

Si usted no quisiera que su router proporcionara ninguna servicios de no ruteo, apagúelo (usando la **ninguna** forma de los comandos anteriores).

Los pequeños servidores TCP son los siguientes:

- ¿**Generación de eco**? Las generaciones de eco apoyan sea cual sea usted teclea. Escriba el comando telnet x.x.x.x echo para ver.
- ¿**Chargen**? Genera un flujo de datos ASCII. Teclee el comando telnet x.x.x.x chargen **de ver**.
- ¿**Deseche**? Descarta todo lo que tipea. Escriba el comando telnet x.x.x.x discard para ver.
- ¿**D3ia**? Devoluciones fecha del sistema y tiempo, si está correcto. Está correcto si usted ejecuta el NTP o ha fijado la fecha y hora manualmente del nivel del ejecutivo. Escriba el comando telnet x.x.x.x daytime para ver.

Los servidores pequeños UDP son:

- ¿**Generación de eco**? Produce eco el payload del datagrama que usted envía.
- ¿**Deseche**? Echa silenciosamente el datagrama que usted envía.

- ¿**Chargen**? Distribuye el datagrama que envíe y responde con una cadena de 72 caracteres ASCII terminada con CR+LF.

Nota: Casi todas las cajas UNIX soportan los pequeños servidores enumerados previamente. El router también ofrece el servicio BOOTP del servicio Finger y de la línea asincrónica. Éstos se pueden apagar independientemente con los comandos configuration global **ningún finger** y **no ip bootp server del servicio**, respectivamente.

Información Relacionada

- Cisco IOS Software
- Soporte Técnico - Cisco Systems