Protéjase contra los ataques de denegación de servicio de puertos de diagnóstico UDP

Contenido

Introducción

Existe un posible ataque de denegación de servicio en los ISP que se dirige a los dispositivos de red.

- **Ataque de puerto de diagnóstico del protocolo de datagramas de usuario (UDP):** Un remitente transmite un volumen de solicitudes de servicios de diagnóstico UDP en el router. Esto hace que se consuman todos los recursos de la CPU para atender las solicitudes falsas.

Este documento describe cómo ocurre el posible ataque de puerto de diagnóstico UDP y sugiere los métodos para utilizar con el software Cisco IOS® para defenderse contra él.

Prerequisites

Requirements

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 a los que se hace referencia en este documento sólo están

disponibles a partir de Cisco IOS Software Releases 10.2(9), 10.3(7) y 11.0(2), y todas las versiones posteriores. Estos comandos son los predeterminados en Cisco IOS Software Release 12.0 y posteriores.

Convenciones

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

Descripción de problemas

Establecimiento del puerto de diagnóstico UDP

De forma predeterminada, el router Cisco tiene una serie de puertos de diagnóstico habilitados para determinados servicios UDP y TCP. Estos servicios incluyen echo, chargen y discard. Cuando un host se conecta a estos puertos, se consume una pequeña cantidad de capacidad de CPU para atender estas solicitudes.

Si un solo dispositivo atacante envía una gran cantidad de solicitudes con diferentes direcciones IP de origen aleatorias falsas, es posible que el router de Cisco se vea saturado y se ralentice o falle.

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 comando exec **show process** muestra muchos procesos con el mismo nombre, como "UDP Echo".

Protéjase de los ataques directamente a los dispositivos de red

Desactivar puertos de diagnóstico UDP

Cualquier dispositivo de red que tenga servicios de diagnóstico UDP y TCP debe estar protegido por un firewall o tener los servicios desactivados. En un router de Cisco esto puede lograrse mediante estos comandos de configuración global.

```
no service udp-small-servers
no 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 los predeterminados en Cisco IOS Software Release 12.0 y posteriores.

Evitar que la red aloje un ataque de forma involuntaria

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 evita el ataque de denegación de servicio en su red. Sin

embargo, ayuda a las partes atacadas a descartar su ubicación como origen del atacante. Además, impide el uso de la red para esta clase de ataques.

Evitar la transmisión de direcciones IP no válidas

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 la red está formada por la red 172.16.0.0 y el router se conecta al ISP mediante una interfaz FDDI0/1, puede aplicar la lista de acceso de la siguiente manera:

```
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 última línea de la lista de acceso determina si hay tráfico con una dirección de origen no válida que entre en Internet. Esto ayuda a localizar el origen de los posibles ataques.

Evitar la recepción de direcciones 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 números de red conectados al router a través de una interfaz FDDI denominada "FDDI 1/0", puede crear esta lista de acceso.

```
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
```

Nota: La última línea de la lista de acceso determina si hay tráfico con una dirección de origen no válida que entre en Internet. Esto ayuda a localizar el origen del posible ataque.

Apéndice: Descripción de servidores pequeños

Los servidores pequeños son servidores (demonios, en lenguaje UNIX) que se ejecutan en el router y que son útiles para el diagnóstico. Por lo tanto, están en funcionamiento por defecto.

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

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

Si no desea que su router proporcione ningún servicio que no sea de ruteo, apáguelos (usando la forma **no** de los comandos anteriores).

Los pequeños servidores TCP son los siguientes:

- **Eco**: reproduce lo que escriba. Escriba el comando telnet x.x.x.x echo para ver.
- **Chargen**: genera una secuencia de datos ASCII. Escriba el comando **telnet x.x.x.x chargen** para ver.
- **Descartar**: tira lo que escriba. Escriba el comando telnet x.x.x.x discard para ver.
- **Daytime**: devuelve la fecha y hora del sistema, si es correcta. Es correcto si ejecuta NTP o ha establecido la fecha y hora manualmente desde el nivel exec. Escriba el comando telnet x.x.x.x daytime para ver.

Los servidores pequeños UDP son:

- **Eco**: hace eco de la carga útil del datagrama que envía.
- **Descartar**: reproduce silenciosamente el datagrama que envía.
- **Chargen**: muestra el datagrama que envía y responde con una cadena de caracteres ASCII de 72 caracteres terminada con un CR+LF.

Nota: Casi todos los equipos UNIX admiten los servidores pequeños enumerados anteriormente. El router también ofrece servicio finger y servicio de inicialización de línea asíncrona. Éstos se pueden desactivar de forma independiente con los comandos de configuración global **no service finger** y **no ip bootp server**, respectivamente.

Información Relacionada

- Cisco IOS Software
- Soporte Técnico - Cisco Systems