Proteja-se contra ataques de negação de serviço de porta de diagnóstico UDP

Contents

Introduction

Há um possível ataque de negação de serviço em ISPs que visa dispositivos de rede.

- **Ataque de porta de diagnóstico do Protocolo de Datagrama de Usuário (UDP - User Datagram Protocol):** Um remetente transmite um volume de solicitações para serviços de diagnóstico UDP no roteador. Isso faz com que todos os recursos da CPU sejam consumidos para atender às solicitações de telefonia.

Este documento descreve como o possível ataque de porta de diagnóstico UDP ocorre e sugere os métodos a serem usados com o software Cisco IOS® para se defender contra ele.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas. Alguns dos comandos mencionados neste documento estão disponíveis somente a partir das versões

10.2(9), 10.3(7) e 11.0(2) do software Cisco IOS e em todas as versões subsequentes. Esses comandos são o padrão no Cisco IOS Software Release 12.0 e posteriores.

Conventions

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

Descrição do problema

O ataque de porta de diagnóstico UDP

Por padrão, o roteador Cisco tem uma série de portas de diagnóstico habilitadas para determinados serviços UDP e TCP. Esses serviços incluem eco, carga e descarte. Quando um host se conecta a essas portas, uma pequena quantidade de capacidade da CPU é consumida para atender a essas solicitações.

Se um único dispositivo de ataque envia uma grande quantidade de solicitações com endereços IP de origem de dados diferentes, aleatórios e falsos, é possível que o roteador Cisco fique sobrecarregado e fique mais lento ou falhe.

A manifestação externa do problema inclui uma mensagem de erro de tabela de processos cheia (%SYS-3 NOPROC) ou uma utilização de CPU muito alta. O comando exec **show process** mostra muitos processos com o mesmo nome, como "UDP Echo".

Defenda-se contra ataques diretamente aos dispositivos de rede

Desativar portas de diagnóstico UDP

Qualquer dispositivo de rede que tenha serviços de diagnóstico UDP e TCP precisa ser protegido por um firewall ou ter os serviços desabilitados. Para um roteador Cisco, isso pode ser feito usando esses comandos de configuração global.

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

Consulte o Apêndice para obter informações sobre estes comandos. Os comando estão disponíveis a partir dos software Cisco IOS versões 10.2(9), 10.3(7) e 11.0(2) e todas as versões subseqüentes. Esses comandos são o padrão no Cisco IOS Software Release 12.0 e posteriores.

Evite que a rede hospede um ataque sem querer

Como um mecanismo primário de ataques de negação de serviço é a geração de tráfego originado a partir de endereços IP aleatórios, a Cisco recomenda filtrar o tráfego destinado para a Internet. O conceito básico é desativar pacotes que tenham endereços IP de origem inválidos quando eles entrarem na Internet. Isso não impede o ataque de negação de serviço em sua rede. No entanto, ajuda as partes atacadas a excluir sua localização como origem do invasor. Além disso, ele impede o uso da rede para essa classe de ataques.

Impedir a transmissão de endereços IP inválidos

Ao filtrar pacotes nos seus roteadores que conectam sua rede à Internet, você pode permitir que apenas pacotes com endereços IP de origem válidos saiam da sua rede e entrem na Internet.

Por exemplo, se sua rede consiste na rede 172.16.0.0 e seu roteador se conecta ao ISP usando uma interface FDDI0/1, você pode aplicar a lista de acesso como esta:

```
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]A última linha da lista de acesso determina se há tráfego com um endereço de origem inválido que entra na Internet. Isso ajuda a localizar a origem dos possíveis ataques.

Evitar recebimento de endereços IP inválidos

Para ISPs que fornecem serviço para redes finais, a Cisco recomenda a validação de pacotes de entrada a partir dos clientes. Isso pode ser obtido pelo uso de filtros de pacotes de entrada nos roteadores de borda.

Por exemplo, se seus clientes tiverem esses números de rede conectados ao roteador por meio de uma interface FDDI chamada "FDDI 1/0", você poderá criar essa lista de acesso.

```
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
```

Observação: a última linha da lista de acesso determina se há tráfego com um endereço de origem inválido que entra na Internet. Isso ajuda a localizar a origem do possível ataque.

Anexo: Descrição de servidores pequenos

Os pequenos servidores são servidores (daemons, em comparação com UNIX) executados no roteador e que são úteis para diagnósticos. Portanto, estão ativados por padrão.

Os comandos para os servidores pequenos de TCP e UDP são:

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

Se você não quiser que o roteador forneça serviços que não sejam de roteamento, desligue-os (usando a forma **no** dos comandos anteriores).

Os pequenos servidores TCP são:

- **Eco** — Ecos de volta o que você digitar. Digite o comando telnet x.x.x.x echo para ver.
- **Chargen** — Gera um fluxo de dados ASCII. Digite o comando **telnet x.x.x.x chargen** para ver.
- **Descartar** — Joga fora o que você digitar. Digite o comando telnet x.x.x.x discard para verificar.
- **Daytime** — Retorna a data e a hora do sistema, se estiverem corretas. É correto que você execute o NTP ou tenha definido a data e a hora manualmente a partir do nível exec. Digite o comando telnet x.x.x.x daytime para ver.

Os pequenos servidores UDP são:

- **Echo** — Eoca o payload do datagrama enviado.
- **Descartar** — Apaga silenciosamente o datagrama enviado.
- **Chargen** — Arredonda o datagrama que você envia e responde com uma sequência de 72 caracteres de caracteres ASCII terminados com um CR+LF.

Observação: quase todas as caixas UNIX suportam os pequenos servidores listados anteriormente. O roteador também oferece serviço finger e serviço de inicialização de linha assíncrona. Eles podem ser desligados independentemente com os comandos globais de configuração **no service finger** e **no ip bootp server**, respectivamente.

Informações Relacionadas

- Cisco IOS Software
- Suporte Técnico - Cisco Systems