防止UDP诊断端口拒绝服务攻击

目录

简介

ISP可能会针对网络设备发起拒绝服务攻击。

- **用户数据报协议 (UDP) 诊断端口攻击**：发送方在路由器上传输大量 UDP 诊断服务请求。这将导致所有 CPU 资源都被用来为这些假冒的请求提供服务。

本文档说明潜在 UDP 诊断端口攻击如何发生，并建议用于 Cisco IOS® 软件以防范攻击的方法。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。本文档中引用的某些命令仅在 Cisco IOS 软件版本 10.2(9)、10.3(7) 和 11.0(2) 及所有后续版本中可用。这些命令在 Cisco IOS 软件版本 12.0 及更高版本中是默认命令。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

问题说明

UDP 诊断端口攻击

默认情况下，Cisco 路由器具有一系列为特定 UDP 和 TCP 服务启用的诊断端口。这些服务包括 echo、chargen 和 discard。当主机连接到这些端口时，将占用少量 CPU 容量来为这些请求提供服务。

如果单个攻击设备源源不断地发送大量具有不同、随机和假冒源 IP 地址的请求，则 Cisco 路由器可能会过载并放慢速度或出现故障。

问题的外部表现包括进程表已满错误消息 (%SYS-3 NOPROC) 或很高的 CPU 使用率。exec 命令 show process 显示大量具有相同名称（如“UDP Echo”）的进程。

保护网络设备免受直接攻击

禁用 UDP 诊断端口

具有 UDP 和 TCP 诊断服务的任何网络设备都需要通过防火墙进行保护或禁用这些服务。对于 Cisco 路由器，这可以通过使用以下全局配置命令来实现。

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

有关这些命令的详细信息，请参阅附录。这些命令在 Cisco IOS 软件版本 10.2(9)、10.3(7) 和 11.0(2) 及所有后续版本中可用。这些命令在 Cisco IOS 软件版本 12.0 及更高版本中是默认命令。

防止网络无意地充当攻击者

由于拒绝服务攻击的主要机制是生成源地址为随机 IP 地址的数据流，因此 Cisco 建议过滤发往 Internet 的数据流。当它们进入互联网时，基本概念是丢掉带有无效源 IP 地址的数据包。这不会阻止您网络上的拒绝服务攻击。但是，它可帮助受到攻击的各方排除将您的位置作为攻击者的源。此外，它还可防止使用您的网络进行此类攻击。

防止传输无效的 IP 地址

在把您的网络连接到互联网的路由器上过滤数据包，您只可以允许带有有效源 IP 地址的数据包离开您的网络，进入互联网。

例如，如果您的网络包括网络 172.16.0.0，而您的路由器使用 FDDI0/1 接口连接到您的 ISP，您可以按如下方式应用访问列表：

```
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]访问列表的最后一行确定是否存在任何源地址无效的流量进入互联网。这可帮助定位可能发起攻击的源。

防止接收无效的 IP 地址

对于向终端网络提供服务的 ISP，Cisco 强烈建议从您的客户端验证传入数据包。这可以通过在边界路由器上使用流入数据包过滤器来实现。

例如，如果您的客户端具有下列通过名为“FDDI 1/0”的 FDDI 接口连接到您的路由器的网络编号，则可创建以下访问列表。

```
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
```
注：访问列表的最后一行确定是否存在任何源地址无效的流量进入互联网。这可帮助定位可能发起攻击的源。

附录：小型服务器说明

小型服务器是在路由器上运行的服务器（在 UNIX 中为后台程序），对诊断十分有用。因此，它们在默认情况下处于打开状态。

用于 TCP 和 UDP 小型服务器的命令包括：

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

如果您不希望您的路由器提供任何非路由服务，请关闭它们（使用前面命令的 **no 形式）。**

TCP 小型服务器包括：

- **回显** — 回显您键入的任何内容。键入命令 **telnet x.x.x.x echo 可进行查看。**
- **Chargen** — 生成ASCII数据流。键入命令 **telnet x.x.x.x chargen 可进行查看。**
- **丢弃** — 丢弃您键入的任何内容。键入命令 **telnet x.x.x.x discard 可进行查看。**
- **Daytime** — 返回系统日期和时间（如果正确）。如果运行 NTP，或者从 exec 级别手动设置日期和时间，则是正确的。键入命令 **telnet x.x.x.x daytime 可进行查看。**

UDP 小型服务器包括：

- **Echo** — 回显您发送的数据报的负载。
- **Discard** — 静默地提出您发送的数据报。
- **Chargen** — 将您发送的数据报提高，并以CR+LF终止的72个ASCII字符字符串作为响应。

注意：几乎所有UNIX机箱都支持之前列出的小型服务器。路由器还提供 finger 服务和异步线路 bootp 服务。使用配置全局命令 **no service finger 和 no ip bootp server 可以分别独立地关闭这些服务。**

相关信息

- Cisco IOS 软件
- 技术支持 - Cisco Systems