链滴

异常网络连接 -UDP 对外反射攻击

作者：yang17762622
原文链接：https://ld246.com/article/1539741524174
来源网站：链滴

今天一大早客户服务器ECS出现问题了

由于某些服务配置不当，导致服务器被黑客利用进行DDoS攻击。具体表现为机器对外带宽占满；使抓包工具检测，可看到大量同一源端口的包对外发出。

提交工单后发现大部分都是UDP放大攻击

Linux解决方案

1. 加固NTP服务

(1).通过Iptables配置只允许信任的IP访问本机UDP的123端口。

修改配置文件，然后执行以下命令：

```
echo "disable monitor" >> /etc/ntp.conf
```

执行以下命令重启NTP服务：

```
service ntpd restart
```

(2)建议直接关闭掉NTP服务，并禁止其开机自启动

执行service ntpd stop命令。
执行chkconfig ntpd off命令。

2. 加固Chargen服务

(1)通过Iptables配置只允许信任的IP访问本机UDP的19端口。

(2)我们建议您直接关闭掉chargen服务。编辑配置文件”/etc/inetd.conf”，用#号注释掉chargen务，然后重启inetd服务

原文链接：异常网络连接 -UDP 对外反射攻击

更多方法请参考ECS反射型DDoS攻击解决方法

原文链接：异常网络连接 -UDP 对外反射攻击