



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

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

今天一大早客户服务器ECS出现问题了

异常网络连接-UDP对外反射攻击

中危 待处理



受影响资产

██████████ 公 |
██████████ 私

源IP

██████████

源PORT

111

目的PORT

5930

攻击类型

SunRPC(PORTMAP)反射攻击

扫描IP频数

2

扫描TCP包频数

1449

持续时间(分钟)

15

事件说明

检测该异常事件意味着您服务器上开启了“Chargen/DNS/NTP/SNMP/SSDP”这些UDP端口服务，黑客通过向该ECS发送伪造源IP和源端口的恶意UDP查询包，迫使该ECS向受害者发起了UDP DDOS攻击。如果这些UDP服务不是您业务场景确实需要，建议及时关闭。

解决方案

建议自查ECS中19、53、123、161、1900 UDP端口是否处于监听状态，如果是非必须开启服务，建议及时关闭。详情可参考：https://help.aliyun.com/knowledge_detail/37527.html

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服务，然后重启inetd服务

更多方法请参考[ECS反射型DDoS攻击解决方法](#)