大家好：

6月19日，爆出了Linux 内核TCP “SACK Panic” 远程拒绝服务漏洞。攻击者可利用该漏洞远程攻击目标服务器，导致系统崩溃或无法提供服务。请各片区尽快通知用户，进行系统内核补丁升级，做好防御工作。

**【高危漏洞预警】Linux 内核TCP “SACK Panic” 远程拒绝服务漏洞**

1. **漏洞情况**

6月19日，爆出了Linux 内核TCP “SACK Panic” 远程拒绝服务漏洞。此次被爆出的是3个DOS漏洞，分别编号为：CVE-2019-11477,CVE-2019-11478,CVE-2019-11479，其中CVE-2019-11477危害最高，攻击者可利用该漏洞远程攻击目标服务器，导致系统崩溃或无法提供服务。

1. **漏洞等级**

**高危**

1. **漏洞影响范围**

**受影响的版本：**

FreeBSD 12（使用到 RACK TCP 协议栈）

CentOS 5（Redhat 官方已停止支持，不再提供补丁）

CentOS 6

CentOS 7

Ubuntu 18.04 LTS

Ubuntu 16.04 LTS

Ubuntu 19.04

Ubuntu 18.10

**升级后详细的安全版本：**

CentOS 6 ：2.6.32-754.15.3

CentOS 7 ：3.10.0-957.21.3

Ubuntu 18.04 LTS ：4.15.0-52.56

Ubuntu 16.04 LTS：4.4.0-151.178

1. **漏洞修复建议**

**1、CentOS 6/7升级方案：**

**注意：此次补丁升级属于系统内核升级，升级可能会导致系统崩溃等异常情况，而且升级成功后也需要重启机器。所以加固前务必做好备份工作，切记！**

注：截止到预警公告发布，CentOS官方暂未同步内核修复补丁到软件源，建议用户及时关注补丁更新情况并开展相应升级工作。升级方式如下：

1). yum clean all && yum makecache，进行软件源更新；

2). yum update kernel  -y，更新当前内核版本;

3). reboot，更新后重启系统生效;

4). uname -a，检查当前版本是否为上述【安全版本】，如果是，则说明修复成功。

**2、Ubuntu 16.04/18.04 LTS升级方案：**

1). sudo apt-get update && sudo apt-get install linux-image-generic，进行软件源更新并安装最新内核版本；

2). sudo reboot，更新后重启系统生效；

3). uname -a，检查当前版本是否为【安全版本】，如果是，则说明修复成功。

**3、临时缓解方案：**

运行如下命令禁用内核 SACK 配置：

sysctl -w net.ipv4.tcp\_sack=0

1. **参考资料**

1、官方通告：

<https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md>

  2、社区参考：

<https://www.openwall.com/lists/oss-security/2019/06/17/5>

  3、红帽公告：

<https://access.redhat.com/security/vulnerabilities/tcpsack>