

升级 Kernel 防御 TCP SACK 漏洞方法

2019 年 6 月 18 日，RedHat 官网发布报告：安全研究人员在 Linux 内核处理 TCP SACK 数据包模块中发现了三个漏洞，CVE 编号为 CVE-2019-11477、CVE-2019-11478 和 CVE-2019-11479。

对于低版本 kernel 内核很有可能被该漏洞利用，可以对内核升级操作。

需自行准备： HTTP 服务器软件。

测试成功的 Linux 版本有：

- CentOS 6.5 (Final)
- Red Hat Enterprise Linux Server release 7.3 (Maipo)

其它 Linux 内核操作系统请自行评估测试！

本次升级需要对操作系统进行重启，如果内核不支持可进行回退，但是必须做好升级的数据备份工作。远程升级有风险！需准备物理屏或

KVM。

修复建议

(1) 及时更新补丁：<https://github.com/Netflix/security-bulletins/tree/master/advisories/third-party/2019-001>。

(2) 禁用 SACK 处理

`echo 0 > /proc/sys/net/ipv4/tcp_sack`

(3) 使用过滤器来阻止攻击

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

此缓解需要禁用 TCP 探测时有效（即在/etc/sysctl.conf 文件中将 net.ipv4.tcp_mtu_probing 设置为 0）

(4) RedHat 用户可以使用以下脚本来检查系统是否存在漏洞

<https://access.redhat.com/sites/default/files/cve-2019-11477--2019-06-17-1629.sh>

参考链接

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

Linux 内核中 TCP SACK 远程拒绝服务漏洞预警

2019 年 6 月 19 日

漏洞编号和级别

CVE 编号: CVE-2019-11477, 危险级别: 高危, CVSS 分值: 厂商自评: 7.5, 官方未评定

CVE 编号: CVE-2019-11478, 危险级别: 中危, CVSS 分值: 官方未评定

CVE 编号: CVE-2019-11479, 危险级别: 中危, CVSS 分值: 官方未评定

影响版本

受影响的版本

影响 Linux 内核 2.6.29 及以上版本

漏洞概述

2019 年 6 月 18 日, RedHat 官网发布报告: 安全研究人员在 Linux 内核处理 TCP SACK 数据包模块中发现了三个漏洞, CVE 编号为 CVE-2019-11477、CVE-2019-11478 和 CVE-2019-11479。

CVE-2019-11477 SACK Panic 漏洞通过“在具有较小值的 TCP MSS 的 TCP 连接上发送精心设计的 SACK 段序列”来利用, 这会触发整数溢出。该漏洞能够降低系统运行效率, 并可能被远程攻击者用于拒绝服务攻击, 影响程度严重。

CVE-2019-11478 SACK Slowness 漏洞通过发送“一个精心设计的 SACK 序列来分解 TCP 重传队列”来利用, 而 CVE-2019-11479 漏洞通过发送“具有低 MSS 值的精心制作的数据包”来利用允许攻击者触发 DoS。

CVE-2019-5599 是 CVE-2019-11478 的 FreeBSD 版本, 它使用 RACK TCP 堆栈影响 FreeBSD 12 的安装, 并且可以通过提供“一个精心设计的 SACK 序列来破坏 RACK 发送映射”。

对我国境内使用 Linux 操作系统的服务器进行统计, 结果显示我国境内开放互联网端口的 Linux 服务器数量约为 202 万台。按分布区统计来看, 排名前三的省份是广东省、浙江省和北京市。

环境描述:

服务器: Red Hat Enterprise Linux Server release 7.3 (Maipo)

Kernel: Red Hat Enterprise Linux Server (3.10.0-514.el7.x86_64) 7.3 (Maipo)

服务器 IP: 192.168.10.55

客户机: Windows 10 -1908

客户机 IP: 192.168.10.94

操作步骤:

1、检查操作系统上的组件版本, 确认存在隐患

```
cat: /etc/redhat-access-insights/: Is a directory
[root@localhost ~]# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 7.3 (Maipo)
[root@localhost ~]# ./cve-2019-11477--2019-06-17-1629.sh

This script (v1.0) is primarily designed to detect CVE-2019-11477 on supported
Red Hat Enterprise Linux systems and kernel packages.
Result may be inaccurate for other RPM based systems.

Running kernel: 3.10.0-514.el7.x86_64

This system is Vulnerable

* Running kernel is vulnerable

For more information about this vulnerability, see:
https://access.redhat.com/security/vulnerabilities/tcpsack
```

2、根据自身系统评估，下载稳定版本的 kernel 版本，下载地址：

https://mirrors.tuna.tsinghua.edu.cn/elrepo/kernel/el7/x86_64/RPMS/

本次使用的版本为：kernel-lt-4.4.182-1.el7.elrepo.x86_64.rpm

（内核建议选择 lt 长期支持版本）

Centos 6.5 测试 kernel-lt-4.12.10-1.el6.elrepo.x86_64、kernel-lt-4.4.182-1.el6.elrepo.x86_64 升级成功。

```
[root@yu ~]# uname -r
4.12.10-1.el6.elrepo.x86_64
[root@yu ~]# uname -a
Linux [redacted] 4.12.10-1.el6.elrepo.x86_64 #1 SMP Wed Aug 30 15:09:18 EDT 2017 x86_64 x86_64 x86_64 GNU/Linux
[root@yu ~]#
```

注意：如果是 6.x 版本系统请下载 el6 内核！

2.1、Yum 源更新

<https://www.elrepo.org/RPM-GPG-KEY-elrepo.org>

下载 key

更新 yum，需要 elrepo-release-7.0-3.el7.elrepo.noarch.rpm

<http://www.elrepo.org/elrepo-release-7.0-3.el7.elrepo.noarch.rpm>

注意：如果是 6.x 版本系统请下载 el6.elrepo

通过各种方式将上述文件上传到服务器上！

3、升级内核需要使用 elrepo 的 yum 源

a、首先我们导入 elrepo 的 key

```
[root@localhost ~]# rpm --import RPM-GPG-KEY-elrepo.org
```

b、安装 elrepo 源

```
[root@localhost ~]# rpm -Uvh elrepo-release-7.0-
```

```
3.el7.elrepo.noarch.rpm
```

```
[root@localhost ~]#  
[root@localhost ~]# rpm --import RPM-GPG-KEY-elrepo.org  
[root@localhost ~]# rpm -Uvh elrepo-release-7.0-3.el7.elrepo.noarch.rpm  
Preparing... ##### [100%]  
Updating / installing...  
 1:elrepo-release-7.0-3.el7.elrepo ##### [100%]  
[root@localhost ~]#
```

4、升级 kernel 内核到相应版本

```
[root@localhost ~]# rpm -Uvh kernel-lt-4.4.182-
```

```
1.el7.elrepo.x86_64.rpm
```

等待 2-3 分钟出现下列提示，内核安装成功！

```
[root@localhost ~]# rpm -Uvh elrepo-release-7.0-3.el7.elrepo.noarch.rpm  
Preparing... ##### [100%]  
Updating / installing...  
 1:elrepo-release-7.0-3.el7.elrepo ##### [100%]  
[root@localhost ~]# rpm -Uvh kernel-lt-4.4.182-1.el7.elrepo.x86_64.rpm  
Preparing... ##### [100%]  
Updating / installing...  
 1:kernel-lt-4.4.182-1.el7.elrepo ##### [100%]  
[root@localhost ~]#
```

5、调整启动 kernel 为升级版本

//CentOS Redhat 7.*版本方法

//确认当前操作系统有几个启动内核，并检查刚刚安装的 kernel 是否存在？

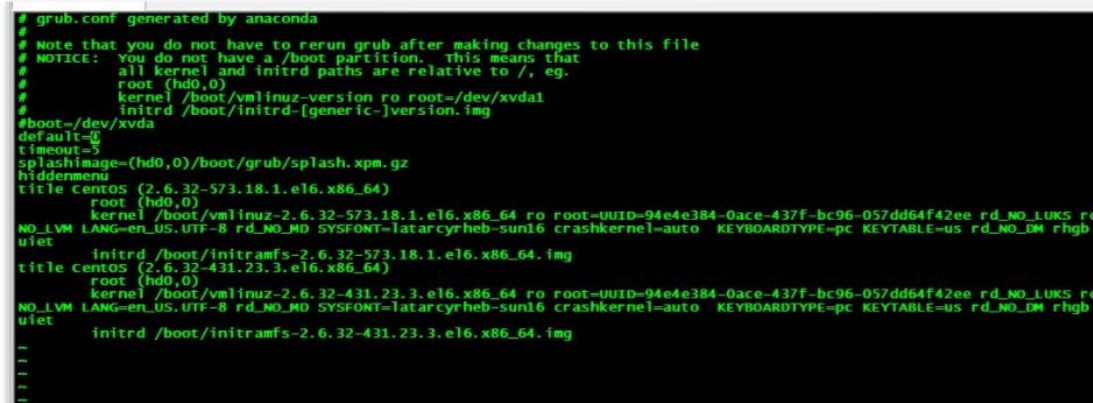
```
[root@server0 ~]# grep "menuentry " /boot/grub2/grub.cfg
```

//选择安装的 kernel 为所要启动

```
[root@server0 ~]# grub2-set-default gnu/linux-3.10.0-514.el7.x86_64-advanced-63b9f6e0-5ae0-4dae-a234-89fef0632876
```

//Redhat CentOS 6.*版本方法

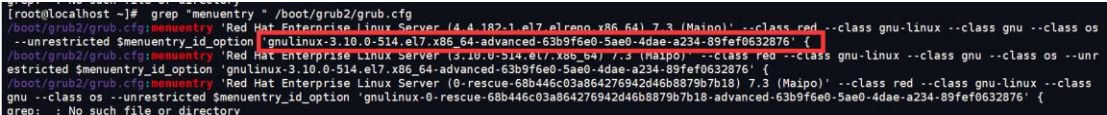
1. vi /etc/grub.conf 查看系统内核的情况，下面的截图是系统存在多个内核的现象：
2. 修改配置步骤：



```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You do not have a /boot partition. This means that
# all kernel and initrd paths are relative to /, eg.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/xvda1
# initrd /boot/initrd-[generic-]version.img
#boot=/dev/xvda
default=0
timeout=5
splashimage=(hd0,0)/boot/grub/splash.xpm.gz
hiddenmenu
title centos (2.6.32-573.18.1.el6.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-2.6.32-573.18.1.el6.x86_64 ro root=UUID-94e4e384-0ace-437f-bc96-057dd64f42ee rd_NO_LUKS rd
NO_LVM LANG=en_US.UTF-8 rd_NO_MD SYSFONT=latarcyrheb-sun16 crashkernel=auto KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb
quiet
initrd /boot/initramfs-2.6.32-573.18.1.el6.x86_64.img
title centos (2.6.32-431.23.3.el6.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-2.6.32-431.23.3.el6.x86_64 ro root=UUID-94e4e384-0ace-437f-bc96-057dd64f42ee rd_NO_LUKS rd
NO_LVM LANG=en_US.UTF-8 rd_NO_MD SYSFONT=latarcyrheb-sun16 crashkernel=auto KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb
quiet
initrd /boot/initramfs-2.6.32-431.23.3.el6.x86_64.img
--
--
--
```

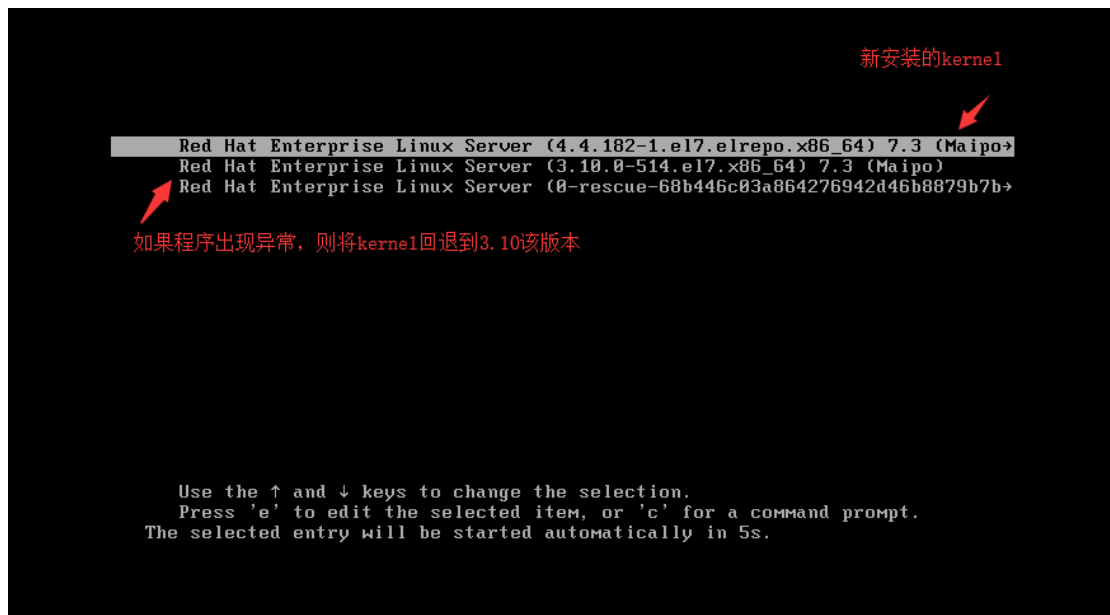
- 1) . 从截图能够看出已经存在两个内核版本，从上往下内核版本依次是 2.6.32-573.18.1.el6.x86_64 和 2.6.32-431.23.3.el6.x86_64。
- 2) . 在 grub.conf 文件中决定开机使用哪个内核版本做启动的参数是 default，默认为 0（代表从最新的内核启动，代表的内核版本从上往下依次是 0，1,2 等）。
- 3.) 在这个例子中，如果要选择从旧版内核即系统最开始的内核启动，则把 default 值改为 1，然后重启服务器从新的内核进行引导。

启动的新 kernel 为红框部分



```
[root@localhost ~]# grep "menuentry" /boot/grub2/grub.cfg
/boot/grub2/grub.cfg:menuentry "Red Hat Enterprise Linux Server (4.4.182-1.el7.elrepo.x86_64) 7.3 (Main0)" --class red --class gnu-linux --class gnu --class os
--unrestricted $menuentry_id_option 'gnulinux-3.10.0-514.el7.x86_64-advanced-63b9f6e0-5ae0-4dae-a234-89fef0632876' {
/boot/grub2/grub.cfg:menuentry "Red Hat Enterprise Linux Server (5.10.0-214.el7.x86_64) 7.3 (Main0)" --class red --class gnu-linux --class gnu --class os --unr
restricted $menuentry_id_option 'gnulinux-3.10.0-514.el7.x86_64-advanced-63b9f6e0-5ae0-4dae-a234-89fef0632876' {
/boot/grub2/grub.cfg:menuentry "Red Hat Enterprise Linux Server (0-rescue-68b446c03a864276942d46b8879b7b10) 7.3 (Maipo)" --class red --class gnu-linux --class
gnu --class os --unrestricted $menuentry_id_option 'gnulinux-0-rescue-68b446c03a864276942d46b8879b7b10-advanced-63b9f6e0-5ae0-4dae-a234-89fef0632876' {
grep: : No such file or directory
```

7、reboot，重新启动服务器，通过 kvm 或屏幕观察是否引导到新的 kernel?



```
Red Hat Enterprise Linux Server (4.4.182-1.el7.elrepo.x86_64) 7.3 (Maipo)
Red Hat Enterprise Linux Server (3.10.0-514.el7.x86_64) 7.3 (Maipo)
Red Hat Enterprise Linux Server (0-rescue-68b446c03a864276942d46b8879b7b)

Use the ↑ and ↓ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
The selected entry will be started automatically in 5s.
```

新安装的kernel

如果程序出现异常，则将kernel回退到3.10该版本

7、执行检查脚本，提示 “Not affected”

```
[root@localhost ~]# ./cve-2019-11477--2019-06-17-1629.sh

This script (v1.0) is primarily designed to detect CVE-2019-11477 on supported
Red Hat Enterprise Linux systems and kernel packages.
Result may be inaccurate for other RPM based systems.

Running kernel: 4.4.182-1.el7.elrepo.x86_64

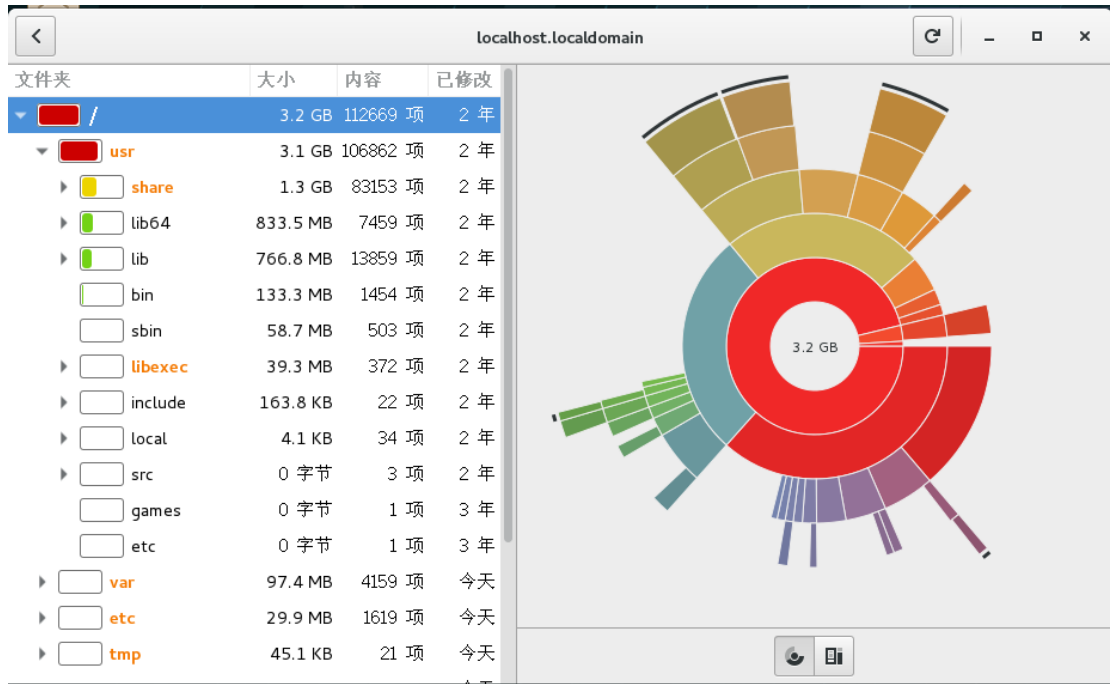
This system is Not affected

For more information about this vulnerability, see:
https://access.redhat.com/security/vulnerabilities/tcpsack
```

新的 kernel 被成功引导启动!

```
[root@localhost ~]# uname -r
4.4.182-1.el7.elrepo.x86_64
[root@localhost ~]#
```

11、再次对服务器复查，业务是否正常！如果业务出现问题，则回退到老版本 kernel。



•需要说明的是安装新内核是占用/boot 空间的,可以使用 yum remove

kernel*** 方式清理不用的 kernel

```
[root@localhost ~]# yum remove kernel-
kernel-3.10.0-514.el7.x86_64 kernel-tools-libs.x86_64
kernel-rt-4.4.182-1.el7.elrepo.x86_64 kernel-tools.x86_64
[root@localhost ~]# yum remove kernel-3.10.0-514.el7.x86_64
```