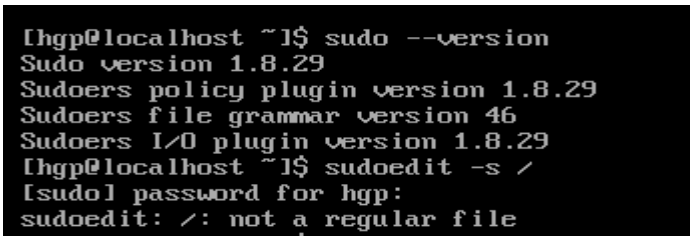
关于 Linux+sudo 权限提升漏洞的预警通知

校属各单位：

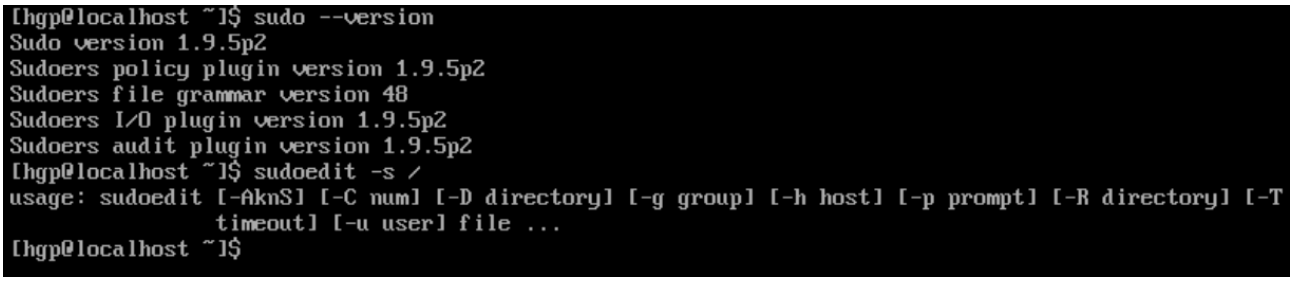
根据上级部门监测发现，Linux Sudo 程序存在堆溢出高危漏洞（漏洞编号：CVE-2021-3156），普通用户可利用此漏洞，在默认配置的 sudo 主机上获取 root 权限控制服务器。相关情况如下：

一、**漏洞介绍**：Sudo 是一款使用于类 Unix 系统的，允许用户通过安全的方式使用特殊的权限执行命令的程序。大多数基于 Unix 和 Linux 的操作系统都包含 Sudo。受影响的版本包括 Sudo1.8.2 到 1.8.31p2 所有版本，Sudo1.9.0 到 1.9.5p1 所有稳定版。

二、**检查方法**：以非 root 账户登录系统运行“sudoedit -s /”命令，受影响的系统启动程序会提示以“sudoedit：”开头的错误作为响应；



安装补丁后启动会出现“usage：”开头的错误提示。如下图：



三、**整改建议**：目前 Sudo 官方已发布安全通告，在新版本 1.9.5p2 中修复了该漏洞，官方下载链接：https://www.sudo.ws/stable.html#1.9.5p2。

四、**升级方法**（以 Centos 为例）：

1.准备工作：

安装补丁前，请先安装 gcc 和 wget,若已经安装,可以忽略。

2. 安装:

切换到需要下载软件的目录，下载最新版本并解压

[root@localhost soft]# wget https://www.sudo.ws/dist/sudo-1.9.5p2.tar.gz

&& tar zxf sudo-1.9.5p2.tar.gz

执行配置命令

[root@localhost soft]# cd sudo-1.9.5p2 && ./configure --prefix=/usr --libexecdir=/usr/lib --with-secure-path --with-all-insults --with-env-editor --docdir=/usr/share/doc/sudo-1.9.5p2 --with-passprompt="[sudo] password for %p: "

编译安装

[root@localhost sudo-1.9.5p2]# make && make install && ln -sfv libsudo_util.so.0.0.0 /usr/lib/sudo/libsudo_util.so.0

以上安装方法仅供参考，不一定适用于所有操作系统版本，如有问题请在官网 https://www.sudo.ws 或百度中查询。

请各单位立即组织专业力量对管理的信息系统服务器开展网络安全风险排查，及时更新漏洞补丁，消除安全隐患。

特此通知。

联系人：侯国平，联系电话：65362000

信息技术中心

2021 年 3 月 1 日