安全漏洞通告

【更新:EXP 公开】CVE-2021-3156：Sudo 堆缓冲区溢出漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-01-27

报告信息

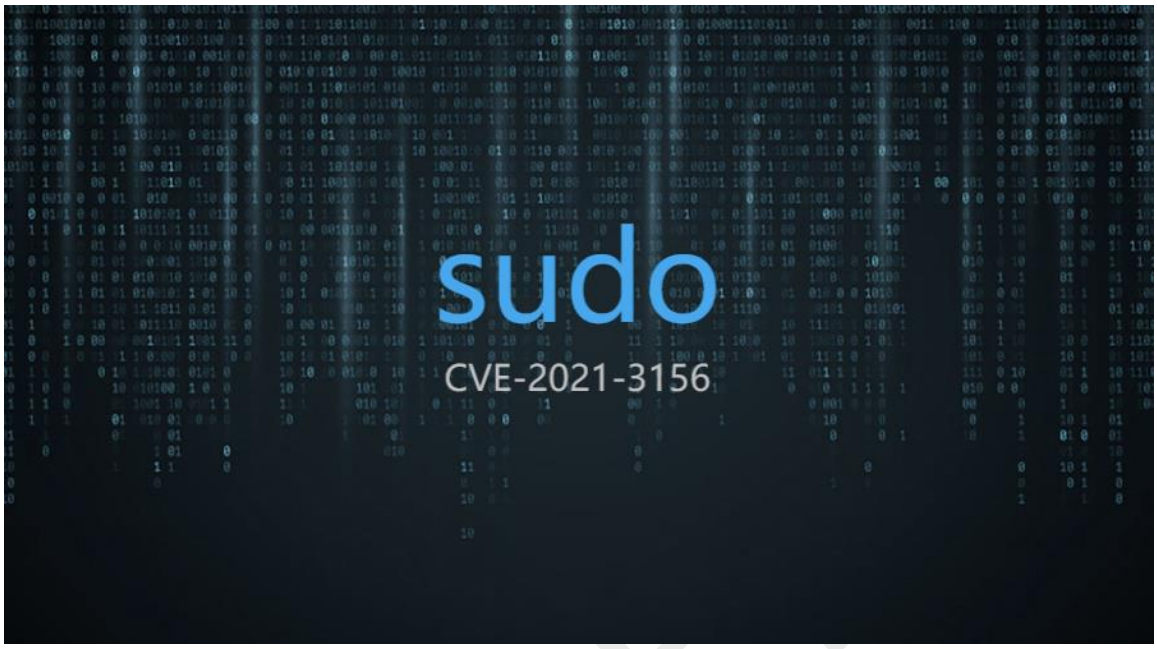
报告名称	【更新:EXP 公开】CVE-2021-3156：Sudo 堆缓冲区溢出漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-020102
报告版本	1	**报告日期**	2021-01-27
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
2	2021-02-01	360CERT	360CERT	撰写报告

目录

一、 漏洞档案



漏洞类型	缓冲区/栈溢出漏洞
CVE 编号	CVE-2021-3156
相关厂商	Sudo
相关组件	暂无
威胁等级	高危
影响面	广泛
360CERT 评分	7.0
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-01-27
报告生成时间	2021-01-27

二、 漏洞简述

2021 年 01 月 30 日，360CERT 监测发现安全研究员 blasty 公开了 CVE-2021-3156 漏洞利用代码。本次更新漏洞状态及复现截图。具体更新详情可参考漏洞详情。2021 年 01 月 27 日，360CERT 监测发现 RedHat 发布了 sudo 缓冲区/栈溢出漏洞 的风险通告，该漏洞编号为 CVE-2021-3156 ，漏洞等级：高危，漏洞评分：7.0。

攻击者在取得服务器基础权限的情况下，可以利用 sudo 基于堆的缓冲区溢出漏洞，获得 root 权限。

目前主流的 Linux 发行版都已经完成该漏洞的修复

对此，360CERT 建议广大用户及时将 sudo 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	高危
影响面	广泛
360CERT 评分	7.0

四、 漏洞详情

CVE-2021-3156: 缓冲区溢出漏洞

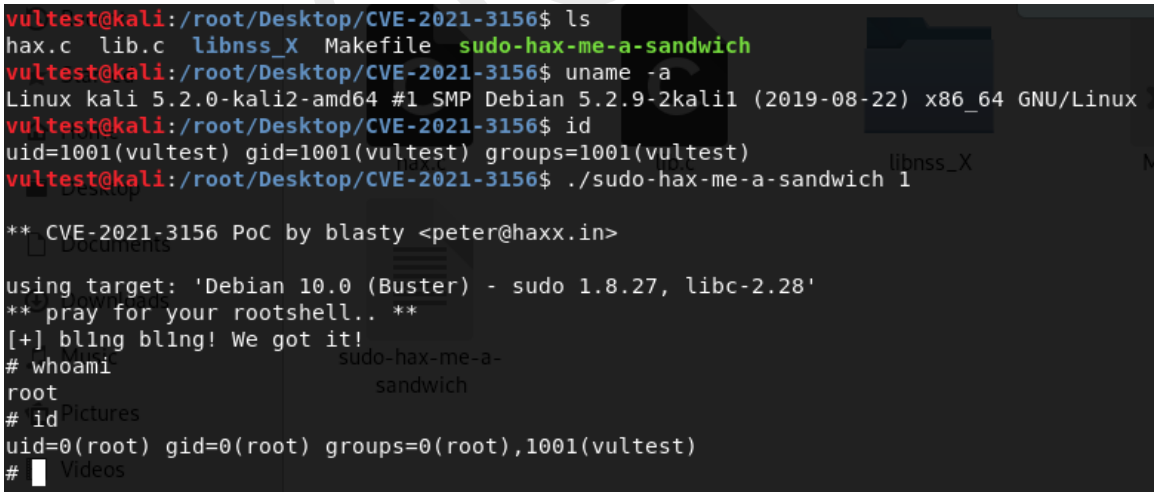
在 sudo 解析命令行参数的方式中发现了基于堆的缓冲区溢出。任何本地用户（普通用户和系统用户，sudoer 和非 sudoers）都可以利用此漏洞，而无需进行身份验证，攻击者不需要知道用户的密码。成功利用此漏洞可以获得 root 权限。

用户可以使用如下方法进行自查:

以非 root 用户登录系统，并使用命令 sudoedit -s /- 如果响应一个以 sudoedit: 开头的报错，那么表明存在漏洞。

- 如果响应一个以 usage: 开头的报错，那么表明补丁已经生效。

目前 360CERT 利用公开的 exp，已经成功复现该漏洞，复现截图如下:



五、 影响版本

产品名称	影响版本
sudo	1.8.2 - 1.8.31p2
sudo	1.9.0 - 1.9.5p1

六、 安全建议

(一) 通用修补方案

下载升级 sudo 软件包，下载链接为：

https://www.sudo.ws/dist/

(二) 临时修补方案

对于无法立即更新的用户，建议使用 systemtap 进行以下临时缓解：

1. 安装所需的 systemtap 软件包和依赖项：

```
systemtap yum-utils kernel-devel-"$(uname -r)"
```

对于 RHEL 7，使用命令安装 kernel debuginfo：debuginfo-install -y kernel-"$(uname -r)"。 对于 RHEL 8，使用命令安装 sudo debuginfo：debuginfo-install sudo。

2. 创建以下 systemtap 脚本（将文件命名为 sudoedit-block.stap）：

```
probe process("/usr/bin/sudo").function("main") {
        command = cmdline_args(0,0,"");
        if (strpos(command, "edit") >= 0) {
                raise(9);
        }
}
```

3. 使用以下命令安装脚本：（使用 root 权限）

```
# nohup stap -g sudoedit-block.stap &
```

该脚本将使得易受攻击的 sudoedit 二进制文件停止工作。 sudo 命令仍将照常工作。上述更改在重启后失效，必须在每次重启后重新应用。

4. 一旦安装了补丁程序，就可以通过取消 systemtap 进程来删除 systemtap 脚本。 例如，通过使用：

```
# kill -s SIGTERM 7590 (其中 7590 是 systemtap 进程的 PID)
```

七、 参考链接

1. RedHat 官方通告

   https://access.redhat.com/security/cve/CVE-2021-3156

2. CVE-2021-3156: Heap-Based Buffer Overflow in Sudo (Baron Samedit)

   https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit

3. CVE-2021-3156 EXP

   https://github.com/blasty/CVE-2021-3156

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危