Sudo 缓冲区溢出漏洞（CVE-2021-3156）修复记录

作者：Jireh

原文链接：https://ld246.com/article/1611824391516

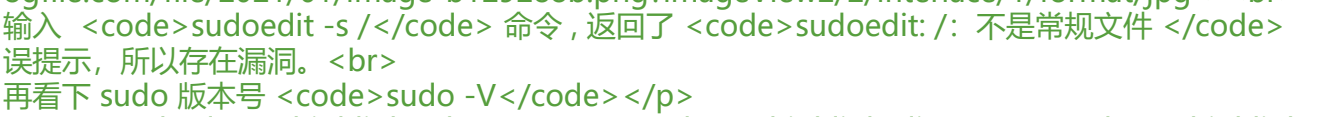
来源网站：链滴

许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

<blockquote>
漏洞名称： Sudo 缓冲区溢出漏洞（CVE-2021-3156）
漏洞定级：高 危
漏洞描述： 在 sudo 中发现一个缺陷。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，sudoers 和非 sudoers）都可以利用此漏洞，而无需进行身份证（即，攻击者不需要知道用户的密码），利用此漏洞可以用于普通用户无差别提权，漏洞对数据机性和完整性以及系统可用性带来严重威胁。
影响范围：
sudo: 1.8.2 - 1.8.31p2
sudo: 1.9.0 - 1.9.5p1
</blockquote>
<h2 id="自查方法">自查方法</h2>
<blockquote>
以非 root 用户登录系统，并使用命令 <code>sudoedit -s /</code>

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。

</blockquote>
<h2 id="处置方法">处置方法</h2>
<blockquote>
通用修补建议： （注意：redhat 可用最新 yum 更新，其他可用包更新的系统也可以尝试）
下载升级 sudo 软件包，下载链接为：>
sudo 软件包下载地址
<a href="https://ld246.com/forward?goto=https%3A%2F%2Fwww.sudo.ws%2Fdist%2F" targe
="_blank" rel="nofollow ugc">https://www.sudo.ws/dist/
</blockquote>
<h3 id="修复记录">修复记录</h3>

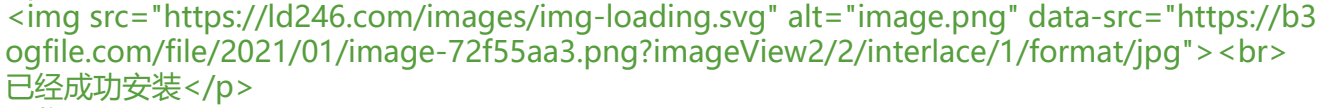
首先查一下是否该漏洞，登录到非 root 用户

输入 <code>sudoedit -s /</code> 命令，返回了 <code>sudoedit: /：不是常规文件 </code>
误提示，所以存在漏洞。
再看下 sudo 版本号 <code>sudo -V</code>
<pre><code class="highlight-chroma"><span class="highlight
cl">[zhyw@localhost ~]$ sudo -V
Sudo 版本 1.8.23
Sudoers 策略插件
本 1.8.23
Sudoers 文件语法
本 46
Sudoers I/O plugi
version 1.8.23
</code></pre>
版本为：1.8.23，的确也是在官方公布的影响范围内的版本

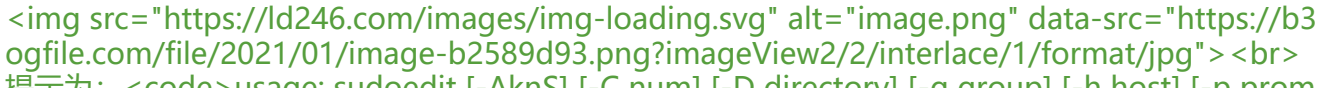
升级修补漏洞，
<code>wget https://www.sudo.ws/dist/sudo.tar.gz</code>

解压

<code>tar -xvzf sudo.tar.gz</code>

进入该文件夹，编译安装
<code>./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: " && make && make install && ln -sfv libsudo_util.so.0.0.0 /usr/lib/sudo/libsudo_util.so.0</code>

再次输入 <code>sudo -V</code> 查看其版本

已经成功安装

验证漏洞是否修复
<code>sudoedit -s /</code>

提示为：<code>usage: sudoedit [-AknS] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] file ... </code>
表示该漏洞已经被修复。

Tip：如果相应的软件源已经更新了 sudo，也可以直接通过 yum 或者 apt-get 来直接升级 <code>yum -y upgrade sudo</code>