Sudo 权限提升漏洞（CVE-2023-22809）通告

■ **通告编号** **NS-2023-00**	■ 发布日期 **2023-03-30**
■ **漏洞危害** **攻击者利用漏洞可实现权限提升**	
■ **TAG** Sudo、权限提升、CVE-2023-22809	

一. 漏洞概述

近日，绿盟科技 CERT 监测发现网上公开披露了 Sudo 权限提升漏洞（CVE-2023-22809）的分析文章与 ExP。由于 Sudo 中的 sudoedit 对处理用户提供的环境变量（如 SUDO_EDITOR、VISUAL 和 EDITOR）中传递的额外参数存在缺陷。当用户指定的编辑器包含绕过 sudoers 策略的“--”参数时，拥有 sudoedit 访问权限的本地攻击者可通过将任意条目附加到要处理的文件列表中，最终在目标系统上实现权限提升。除外，该漏洞还影响部分 QNAP 操作系统：QTS、QuTS hero、QuTScloud、QVP（QVR Pro 设备）。经综合判断，该漏洞仅影响添加了特定配置的客户，影响范围比较有限，请相关用户根据自身实际情况进行防护。

参考链接：

https://www.openwall.com/lists/oss-security/2023/01/19/1

https://www.qnap.com/en/security-advisory/qsa-23-11

二. 影响范围

受影响范围

Sudo：

- 1.8.0 <= Sudo <= 1.9.12p1

QTS 与 QuTS hero：

- QTS < 5.0.1.2346 build 20230322
- QuTS < hero h5.0.1.2348 build 20230324

不受影响范围

Sudo：

- Sudo >= 1.9.12.p2

注：Sudo 1.8.0 之前不受该漏洞影响

QTS 与 QuTS hero：

- QTS >= 5.0.1.2346 build 20230322
- QuTS >= hero h5.0.1.2348 build 20230324

三. 漏洞检测

3.1 版本检测

相关用户可通过版本检测的方式判断当前应用是否存在风险。可通过以下命令查看当前版本。

```
sudo -V
```

若版本在受影响范围内则可能存在安全风险。

四. 漏洞防护

4.1 官方升级

1. 目前官方已发布新版本修复此漏洞，建议受影响的用户及时安装防护：

   https://www.sudo.ws/releases/stable/

2. 目前主流 Linux 发行版均已发布安全补丁或更新版本修复此漏洞，建议用户尽快安装补丁或参照官方措施进行防护：

Linux 发行版	官方通告
Ubuntu	https://ubuntu.com/security/CVE-2023-22809
Debain	https://security-tracker.debian.org/tracker/CVE-2023-22809
Redhat	https://access.redhat.com/security/cve/CVE-2023-22809
Gentoo	https://bugs.gentoo.org/show_bug.cgi?id=CVE-2023-22809
Mageia	https://advisories.mageia.org/CVE-2023-22809.html

注：如 Ubuntu、Debian、CentOS 等使用包管理器更新 Sudo 的 Linux 发行版，可直接运行下列命令进行更新修复：

Ubuntu、Debian：

```
sudo apt-get update
sudo apt-get upgrade
```

CentOS：

```
sudo yum update sudo
```

3. 受影响的 QNAP 系统：QTS、QuTS hero、QuTScloud、QVP（QVR Pro 设备），修复方案详情请参考以下链接：

https://www.qnap.com/en/security-advisory/qsa-23-11

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。