OpenSSH 命令注入漏洞（CVE-2023-51385）通告

■ 通告编号 **NS-2023-00**	■ 发布日期 **2023-12-25**
■ 漏洞危害	攻击者利用此漏洞，可实现任意命令执行。
■ **TAG**	OpenSSH、ProxyCommand、CVE-2023-51385

一. 漏洞概述

近日，绿盟科技 CERT 监测到 OpenSSH 发布安全更新，修复了一个恶意 Shell 字符导致的命令注入漏洞（CVE-2023-51385），CVSS 评分为 9.8；由于在 OpenSSH 的 ProxyCommand 命令中未对%h，%u 表示的用户名和主机名输入进行安全过滤，如果用户名或主机名中含有 shell 元字符（如 | ' "等），并且 ssh_config 中 ProxyCommand、LocalCommand 指令或"match exec"通过%h，%u 等扩展标记引用了用户或主机名时，可能会发生命令注入。常见攻击场景：一个不受信任的 Git 仓库包含用户或主机名中的 shell 元字符，当用户递归更新该仓库时则会触发漏洞执行。目前 PoC 已公开，请受影响的用户尽快采取措施进行防护。

OpenSSH 是 SSH （Secure SHell） 协议的免费开源实现。SSH 协议族可以用来进行远程控制， 或在计算机之间传送文件。

参考链接：

https://www.openssh.com/txt/release-9.6

二. 影响范围

受影响版本

- OpenSSH < 9.6

不受影响版本

- OpenSSH >=9.6/9.6p1

三. 漏洞检测

3.1 人工检测

由于更新 OpenSSH 版本可能会有新老版本共存的情况，为保证版本检测的准确性，用户可使用如下命令查看当前使用的 OpenSSH 版本，判断是否在影响范围内：

```
ssh -V
```

```
[root@localhost Desktop]# ssh -V
OpenSSH_5.3p1, OpenSSL 1.0.1e-fips 11 Feb 2013
[root@localhost Desktop]#
```

四. 漏洞防护

4.1 官方升级

目前官方已在最新版本中修复了该漏洞，请受影响的用户尽快升级版本进行防护，官方下载链接： https://www.openssh.com/releasenotes.html

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。