**南开大学**

**实习实训漏洞复现报告**

**2024年7月25日**

目录

[1.漏洞复现结论（15分） 1](#_Toc28487)

[1.1风险等级分布 1](#_Toc7481)

[2.工作计划（25分） 1](#_Toc24528)

[2.1工作人员 1](#_Toc13939)

[2.2漏洞对象 1](#_Toc3137)

[2.3漏洞复现阶段 1](#_Toc7909)

[2.4风险等级 2](#_Toc1860)

[3.漏洞复现过程（35分） 2](#_Toc6133)

[3.1 风险管理及规避 2](#_Toc18532)

[3.2测试方法 2](#_Toc4033)

[3.3测试中所用的工具 2](#_Toc28445)

[4. 漏洞复现结果（25分） 3](#_Toc12892)

[4.1 POC插件编写 3](#_Toc32666)

[4.2 漏洞信息 3](#_Toc25120)

# 1.漏洞复现结论（15分）

南开大学15小组的安全人员采用科学的漏洞复现步骤于2024年7月15日至2024年7月25日对Git凭证泄露进行了全面深入的漏洞复现。

本次共发现漏洞1个，其高危漏洞1个，中危漏洞0个,低危漏洞0个。

|  |  |  |
| --- | --- | --- |
| **序号** | **漏洞名称** | **风险值** |
| 1 | Git凭证泄露（CVE-2020-5260） | 高危 |

## 1.1风险等级分布

本次评估漏洞的详细风险等级分布如下：

高危

# 2.工作计划（25分）

## 2.1工作人员

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 职务 | 姓名 | 联系方式 |
| 1 | 组长 | 常欣然 | 1195108945@qq.com |
| 2 | 组员 | 高玉格 | 1463948484@qq.com |
| 3 | 组员 | 马浩博 | 1191173636@qq.com |
| 4 | 组员 | 宋常秀 | 3281405348@qq.com |
| 5 | 组员 | 曹瑜 | 463246828@qq.com |

## 2.2漏洞对象

Git

## 2.3漏洞复现阶段

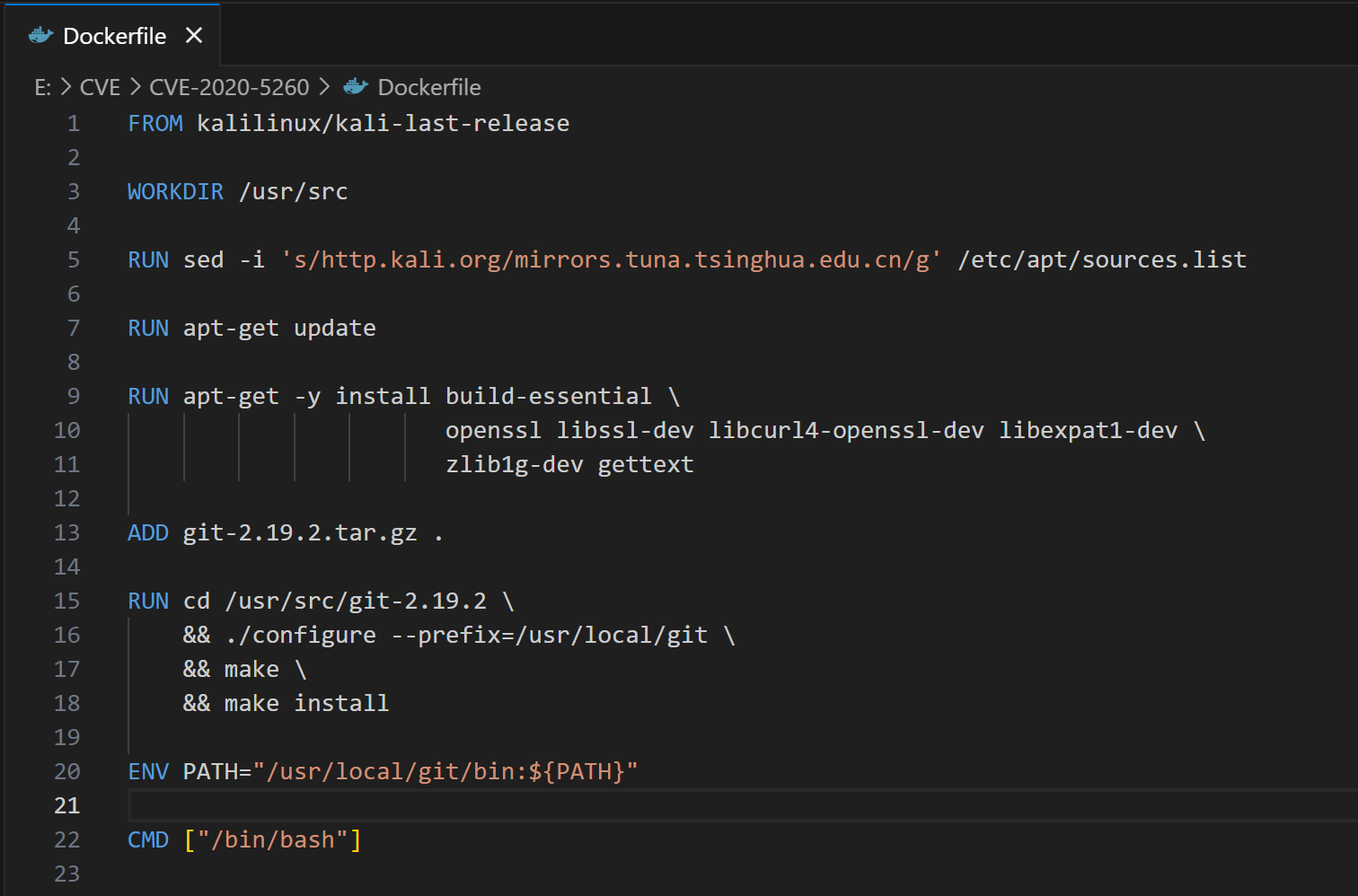
|  |  |
| --- | --- |
| 项目阶段 | 工作内容 |
| 环境搭建 | 使用Docker编写dockerfile进行环境搭建 |
| 版本检测 | 观察git的版本是否在受影响的范围内 |
| Poc验证 | 运行poc脚本 |

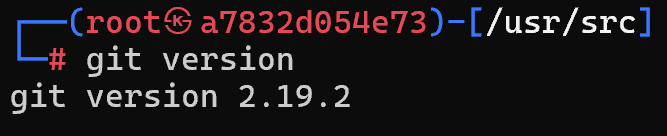
## 2.4风险等级

|  |  |  |
| --- | --- | --- |
| 编号 | 风险等级 | 风险描述 |
| 1 | 高危 | 攻击者利用此漏洞可使恶意URL欺骗Git客户端向攻击者发送主机凭据 |

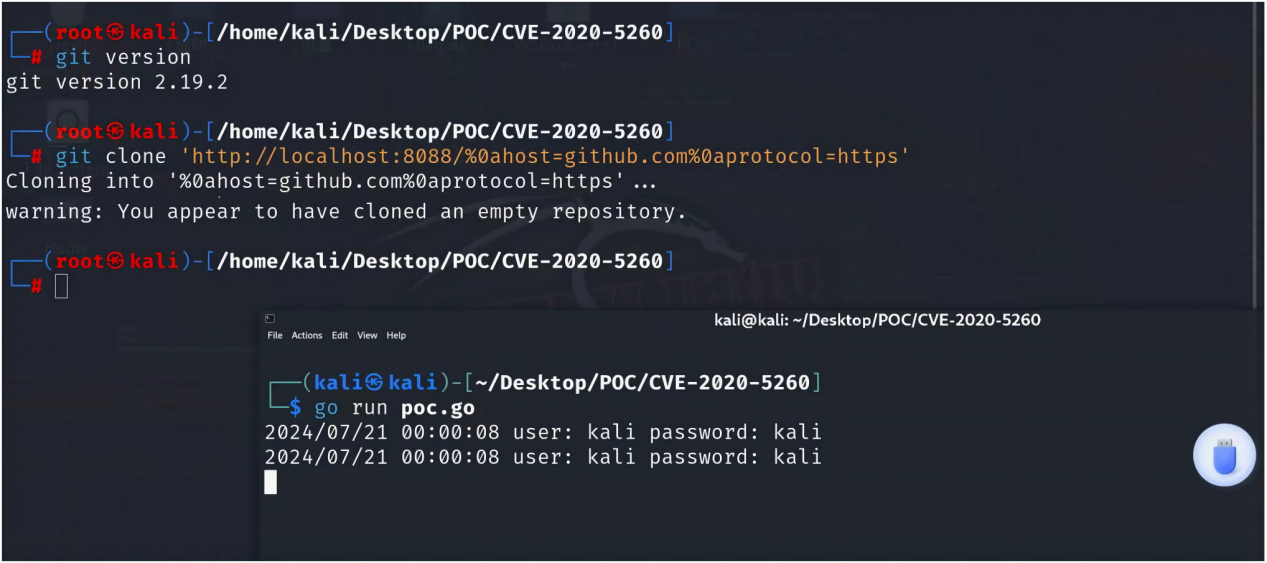
# 3.漏洞复现过程（35分）

1. 使用Docker，编写dockerfile进行环境搭建



1. 在命令行中使用git version命令观察git的版本是否在受影响的范围内：

发现在影响范围内，运行poc脚本进行检测：



输入payload后，可以发现在漏洞环境中输入的用户名与密码重要信息回被泄露，显示在脚本窗口中，说明确实存在凭证泄露漏洞。

## 3.1 风险管理及规避

（1）官方升级：目前官方已在最新版本中修复了该漏洞，受影响的用户尽快升级版本进行防护；

（2）使用以下命令禁用credential helper：

git config --unset credential.helper

git config --global --unset credential.helper

git config --system --unset credential.helper

（3）检查git clone的URL，避免子模块与不受信仓库一起使用，不执行对不信任URL的git clone。

## 3.2测试方法

Poc验证

## 3.3测试中所用的工具

有漏洞版本的git用来搭建环境：git-2.19.2

VSCode：编写dockerfile即poc脚本

Docker Desktop：创建运行docker容器

# 漏洞复现结果（25分）

## POC插件编写

cve-2020-5260-poc

cve-2020-5260-Dockerfile

## 4.2 漏洞信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **UVD-ID** |  | **漏洞类别** | 不充分的凭证保护机制（CWE-522） | **CVE-ID** | CVE-2020-5260 |
| **披露/发现时间** | 2020-04-15 | **bugtraq编号** |  | **CNNVD-ID：** |  |
| **提交时间** | 2023-11-05 | **漏洞发现者** | Git官方 | **CNVD-ID：** |  |
| **漏洞等级** | 低危 | **提交者** | Git官方 | **搜索关键词** | Git凭证泄露 |
| **影响范围** | 受影响版本：  Git 2.17.x <= 2.17.3  Git 2.18.x <= 2.18.2  Git 2.19.x <= 2.19.3  Git 2.20.x <= 2.20.2  Git 2.21.x <= 2.21.1  Git 2.22.x <= 2.22.2  Git 2.23.x <= 2.23.1  Git 2.24.x <= 2.24.1  Git 2.25.x <= 2.25.2  Git 2.26.x <= 2.26.0  不受影响版本：  Git 2.17.4  Git 2.18.3  Git 2.19.4  Git 2.20.3  Git 2.21.2  Git 2.22.3  Git 2.23.2  Git 2.24.2  Git 2.25.3  Git 2.26.1 | | | | |
| **来源** | 由Git官方发布 | | | | |
| **漏洞简介** | Git使用凭证助手(credential helper)来帮助用户存储和检索凭证。当URL中包含经过编码的换行符（%0a）时，可能将非预期的值注入到credential helper的协议流中。受影响版本 Git对恶意 URL 执行 git clone 命令时会触发此漏洞，攻击者可利用恶意URL欺骗Git客户端发送主机凭据。 | | | | |
| **漏洞详情** | 受影响的Git版本存在一个漏洞，可以诱骗Git向攻击者控制的主机发送私有凭据。 Git使用外部“凭据帮助程序”来存储和检索操作系统提供的安全存储中的密码或其他凭据。包含编码换行符的特制URL可以将意想不到的值注入到凭据帮助程序协议流中，从而导致凭据帮助程序检索一台服务器（例如good.example.com）的密码，以向另一台服务器发出HTTP请求（例如：evil.example.com），从而导致前者的凭据发送到后者。两者之间的关系没有任何限制，这意味着攻击者可以制作一个URL，该URL将向其选择的主机提供任何主机的存储凭据。可以通过向git clone提供恶意URL来触发此漏洞。但是，受影响的URL看起来可疑。可能的媒介是通过自动克隆用户不可见的URL的系统（例如Git子模块）或围绕Git构建的打包系统。 | | | | |
| **参考链接** | <https://cloud.tencent.com/developer/article/1616917>  <https://avd.aliyun.com/detail?id=AVD-2020-5260>  <https://github.com/git/git/security/advisories/GHSA-qm7j-c969-7j4q>  https://gitee.com/src-openeuler/git/issues/I8DPUE | | | | |
| **靶场信息** | 镜像：kalilinux/kali-latest-release  Git：2.19.2 | | | | |
| **POC** | cve-2020-5260-poc.go | | | | |
| **修复方案** | 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。  其他防护措施：  使用以下命令禁用credential helper：  git config --unset credential.helper  git config --global --unset credential.helper  git config --system --unset credential.helper  提高警惕避免恶意URL：git clone时检查URL的主机名和用户名部分是否存在编码的换行符（%0a）或凭据协议注入的证据（例如host=github.com）。避免将子模块与不受信任的仓库一起使用（不要使用clone --recurse-submodules；只有在检查.gitmodules中找到url之后，才使用git submodule update）。请勿对不信任的URL执行git clone。 | | | | |