# 2023-02-15-Git缓冲区溢出 CVE-2022-41903, CVE-2022-23521

## 描述

多个产品中的Git缓冲区溢出

| | |
|---|---|
| **主题** | Git缓冲区溢出 CVE-2022-41903, CVE-2022-23521 |
| **发布日期** | 2023 年 2 月15 日 |
| **产品** | • BitBucket server<br>• Bitbucket DataCenter<br>• Fisheye<br>• Crucible<br>• Sourcetree |
| **CVE ID** | CVE-2022-41903, CVE-2022-23521 |

# 漏洞摘要

## CVE-2022-41903

使用git archive, git log --format

git log能够使用任意格式及其--format说明符显示提交。此功能还通过导出export-subst属性公开给git存档。

当执行用于格式化的填充运算符时（例如，%<（，%<|（，%>（，>>（，或%><（））），可能会发生整数溢出。此溢出可以由用户运行调用提交格式化机制的命令直接触发，也可以通过git存档和导出子机制间接触发。

整数溢出导致任意堆写入，这可能导致远程代码执行，发送恶意 HTTP 请求来执行任意代码。

## CVE-2022-23531

gitattributes解析整数溢出

gitattributes是一种允许为路径定义属性的机制。这些属性可以通过向存储库中添加.gitattributes文件来定义，该文件包含一组文件模式和应为匹配此模式的路径设置的属性。

在分析gitattributes时，当存在大量路径模式、单个模式的大量属性或声明的属性名称巨大时，可能会发生多个整数溢出。这些溢出可以通过可能是提交历史记录一部分的特制.gitattributes文件触发。

此整数溢出可能导致任意的堆读写操作，这可能导致远程代码执行。

## 修复方法

更新服务器中Git的版本，版本要求如下

- >= v2.30.7, v2.31.6, v2.32.5, v2.33.6, v2.34.6, v2.35.6, v2.36.4, v2.37.5, v2.38.3, v2.39.

## 影响产品

BitBucket的数据中心或者服务器版本，可以将Git升级到指定版本

升级Git的时候，需要检查BitBucket版本是否允许 支持以上Git版本

## GIT漏洞说明

- Git Security Advisory - CVE-2022-41903
- Git Security Advisory - CVE-2022-23521