

# GitLab 代码执行漏洞（CVE-2023-2478）

■ 通告编号 NS-2023-00

■ 发布日期 2023-05-08

■ 漏洞危害 低权限的远程攻击者可通过 GraphQL 端点将恶意 Runner 添加到实例的任意项目上，进一步利用可在目标系统上执行任意代码或敏感信息泄露

■ TAG GitLab、CVE-2023-2478、远程代码执行、数据泄露



## 一. 漏洞概述

近日，绿盟科技 CERT 监测到 GitLab 官方发布安全通告，修复了 GitLab 社区版（CE）和企业版（EE）中的一个代码执行漏洞（CVE-2023-2478）。具有低权限的远程攻击者可通过 GraphQL 端点将恶意 Runner 添加到实例的任意项目上，进一步利用可在目标系统上执行任意代码或敏感信息泄露。CVSS 评分为 9.6，请受影响的用户尽快采取措施进行防护。

GitLab 是一个用于仓库管理系统的开源项目，其使用 Git 作为代码管理工具，可通过 Web 界面访问公开或私人项目。

本次更新的漏洞状态：

| 漏洞细节 | 漏洞 PoC | 漏洞 EXP | 在野利用 |
|------|--------|--------|------|
| 未公开  | 未公开    | 未公开    | 暂不存在 |

参考链接：<https://about.gitlab.com/releases/2023/05/05/critical-security-release-gitlab-15-11-2-released/#malicious-runner-attachment-via-graphql>

## 二. 影响范围

受影响版本

- 15.4 <= GitLab CE/EE < 15.9.7
- 15.10 <= GitLab CE/EE < 15.10.6
- 15.11 <= GitLab CE/EE < 15.11.2

不受影响版本

- GitLab CE/EE >= 15.9.7
- GitLab CE/EE >= 15.10.6
- GitLab CE/EE >= 15.11.2

## 三. 漏洞检测

### 3.1 版本检测

相关用户可通过版本检测的方法判断当前应用是否存在风险。

使用如下命令可查看当前使用的 GitLab 版本：

```
cat /opt/gitlab/embedded/service/gitlab-rails/VERSION
```

```
[root@localhost gitlab-rails]# cat /opt/gitlab/embedded/service/gitlab-rails/VERSION  
11.0.6
```

若当前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

目前 GitLab 官方已发布安全版本修复此漏洞，建议受影响的用户及时升级防护：

<https://about.gitlab.com/update/>

## 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。