2022-08-24-Bitbucket-命令行注入漏洞-CVE-2022-36804

描述

Bitbucket 服务器和数据中心 - 命令注入漏洞 - CVE-2022-36804

主题	CVE-2022-36804 - 命令注入漏洞
发布日期	2022 年 8 月 24 日
产品	• BitBucket server • Bitbucket DataCenter
CVE ID	CVE-2022-36804

漏洞摘要

本公告披露了在 Bitbucket Server 和 Data Center 7.0.0 版中引入的严重严重性安全漏洞。在6.10.17之后发布的所有版本（包括 7.0.0 及更高版本）都会受到影响，

所有运行7.0.0 和 8.3.0 （包括）之间任何版本的实例都会受到此漏洞的影响。

Bitbucket Server 和 Data Center 的多个 API 端点存在命令注入漏洞。有权访问公共存储库或对私有 Bitbucket 存储库具有**读取**权限的攻击者可以通过发送恶意 HTTP 请求来执行任意代码。

严重性

根据我们在 Atlassian 严重性级别中发布的等级，Atlassian 将此漏洞的严重性级别评为**严重**。

受影响的版本

所有运行7.0.0 和 8.3.0之间的任何版本的实例都会受到此漏洞的影响。

修复版本

支持的版本	错误修复发布
Bitbucket 服务器和数据中心 7.6	7.6.17 （LTS）或更新版本
Bitbucket 服务器和数据中心 7.17	7.17.10 （LTS）或更新版本
Bitbucket 服务器和数据中心 7.21	7.21.4 （LTS）或更新版本
Bitbucket 服务器和数据中心 8.0	8.0.3 或更新版本
Bitbucket 服务器和数据中心 8.1	8.1.3 或更新版本
Bitbucket 服务器和数据中心 8.2	8.2.2 或更新版本
Bitbucket 服务器和数据中心 8.3	8.3.1 或更新版本

如何修复

建议将实例升级到相应的“修复版本”。

Bitbucket Mesh

如果您已配置 Bitbucket Mesh 节点，则需要将这些节点更新为包含该修复程序的相应 Mesh 版本。可以查看兼容性矩阵。

如果您不确定您的 Bitbucket 实例是否配置了 Bitbucket Mesh，作为具有系统管理权限的用户导航到**Administration > Bitbucket Mesh**，此页面将列出每个需要升级的 Mesh 节点。

如果列表为空，则您的实例未配置 Mesh，不需要此额外步骤。

临时解决方案

如果无法升级 Bitbucket，可以临时进行解决，方案如下

在bitbucket.properties(位置：**{Bitbucket home}/shared/下**)文件中增加以下参数

feature.public.access=false

然后重新 启动BitBucket