安全通告

禅道项目管理系统身份认证绕过

漏洞预警通报

发布日期：2024-6-7

[2024]008 号

漏洞描述

2024 年 6 月 5 日公司监测到禅道项目管理系统身份认证绕过漏洞。禅道是第一款国产的开源项目管理软件，它的核心管理思想基于敏捷方法 scrum，内置了产品管理和项目管理，同时又根据国内研发现状补充了测试管理、计划管理、发布管理、文档管理、事务管理等功能，在一个软件中就可以将软件研发中的需求、任务、bug、用例、计划、发布等要素有序地跟踪管理起来，完整地覆盖了项目管理的核心流程。禅道项目管理系统存在身份认证绕过漏洞，远程攻击者利用该漏洞可以绕过身份认证，调用任意 API 接口并修改管理员用户的密码，并以管理员用户登录该系统，配合其他漏洞进一步利用后，可以实现完全接管服务器。

漏洞编号

DVB-2024-6957

漏洞危害

该漏洞允许未授权用户绕过正常认证流程，创建管理员账户并接管后台，进而可能利用其他后台漏洞实现远程代码执行，严重威胁系统安全，可能导致数据泄露、勒索或更广泛的网络攻击。

漏洞等级

严重

影响范围：

v16.x <= 禅道 < v18.12 （开源版）

v6.x <= 禅道 < v8.12 （企业版）

v3.x <= 禅道 < v4.12 （旗舰版）

修复方案

目前该漏洞已在官方最新版本中进行了更新修复，请相关用户尽快升级到最新版本。

链接如下：

https://www.zentao.net/