

# 泛微 Ecology OA SQL 注入漏洞



**SANGFOR**  
深信服科技



**深信服千里目**  
Sangfor DeepINSight

2023 年 4 月 22 日

## 一、漏洞概要

漏洞名称	泛微 Ecology OA SQL 注入漏洞
发布时间	2023 年 4 月 22 日
组件名称	泛微 Ecology
影响范围	泛微 Ecology 9.x 补丁版本号 <= v10.56 泛微 Ecology 8.x 补丁版本号 <= v10.56
漏洞类型	SQL 注入
利用条件	1、用户认证：否 2、前置条件：无 3、触发方式：远程
综合评价	<综合评定利用难度>：未知 <综合评定威胁等级>：高危，能造成信息泄露。
官方解决方案	已发布

## 二、漏洞分析

### 2.1 组件介绍

泛微协同管理应用平台(E-Cology)是一套兼具企业信息门户、知识文档管理、工作流程管理、人力资源管理、客户关系管理、项目管理、财务管理、资产管理、供应链管理、数据中心功能的企业大型协同管理平台。

### 2.2 漏洞描述

2023年4月22日,深信服安全团队监测到一则泛微 E-Cology 组件存在 SQL 漏洞的信息,漏洞威胁等级:高危。

该漏洞是由于泛微 Ecology 系统对用户传入的数据过滤处理不当,导致存在 SQL 注入漏洞,远程且未经过身份认证的攻击者可利用此漏洞进行 SQL 注入攻击,从而可窃取数据库敏感信息。

### 三、影响范围

目前受影响的泛微 Ecology 版本：

泛微 Ecology 9.x 补丁版本号  $\leq$  v10.56

泛微 Ecology 8.x 补丁版本号  $\leq$  v10.56

深信服千里目安全技术中心

## 四、解决方案

### 4.1 修复建议

#### 1.官方修复建议

当前官方已发布最新补丁,建议受影响的用户及时更新升级到最新补丁版本。链接如下:

<https://www.weaver.com.cn/cs/securityDownload.html?src=cn>

## 五、时间轴

2023/4/22 深信服监测到泛微 Ecology 官方发布安全通告。

2023/4/22 深信服千里目安全技术中心发布漏洞通告。

深信服千里目安全技术中心

## 六、参考链接

<https://www.weaver.com.cn/cs/securityDownload.html?src=cn>

深信服千里目安全技术中心

## 七、了解更多

深信服千里目安全技术中心持续紧跟国内外漏洞威胁情报，从中筛选出能给客户带来威胁的漏洞，第一时间推送解决方案，持续提供可感知的安全感。在这场永不停歇的攻防战争中，深信服千里目安全技术中心掌握一手漏洞情报，坚持“千里之外，洞悉风险”，与各大网络安全厂商一同维护网络安全，构建平衡、和谐的网络生态系统。关注深信服千里目安全技术中心微信公众号，第一时间了解更多漏洞情报。

