河南省教育信息安全监测中心
关于泛微 e-cology 协同管理应用平台
存在文件上传漏洞的情况通报

2024 年 05 月 31 日

关于泛微 e-cology 协同管理应用平台存在文件上传漏洞的情况通报

漏洞背景

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。支持 OA、CRM、ERP 等多种业务应用系统，并提供了完善的权限控制、数据加密保护机制，以及灵活的定制化开发方案。

漏洞描述

工作发现，泛微网络科技股份有限公司 e-cology 协同管理应用平台存在文件上传漏洞。由于该平台 SkinAction 接口对用户提交的数据检验不严，导致攻击者可以绕过安全检验提交修改过的数据，进而获取服务器 Webshell 权限。漏洞影响 e-cology 大部分版本。

漏洞编号

无

影响范围

大部分版本

漏洞危害

高危

安全建议

鉴于境外黑客组织频繁对我协同办公类软件实施网络攻击请各单位高度重视，迅速开展以下工作：

1、立即排查本单位泛微 e-cology 协同管理应用平台使用情况；

2、密切关注厂商漏洞补丁发布情况，及时消除风险隐患。补丁发布前可在确保安全的前提下，采取对用户上传的文件进行严格输入验证和过滤、限制上传文件存储位置和访问权限、使用安全的文件处理函数和 API 等临时性措施；

泛微安全中心网站：

https://www.weaver.com.cn/news/src/

3、加强网络安全监测，如发现遭攻击情况及时处置报告。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052