河南省教育信息安全监测中心

泛微 OA 系统 SQL 注入漏洞预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2019 年 10 月 12 日

泛微 E-cology OA 系统 SQL 注入漏洞

事件描述

泛微 E-cology OA 系统是一套兼具企业信息门户、知识管理、数据中心、工作流管理、人力资源管理、客户与合作伙伴管理、项目管理、财务管理、资产管理功能的协同商务平台。泛微 e-cology OA 系统的 WorkflowCenterTreeData 接口在使用 Oracle 数据库时,由于内置 SQL 语句拼接不严格,导致泛微 e-cology OA 系统存在 SQL 注入漏洞。攻击者利用该漏洞，可在未授权的情况下，远程发送精心构造的 SQL 语句，从而获取数据库敏感信息。

漏洞编号

CNNVD-201910-647

影响范围

成功利用此漏洞的攻击者，可以远程获取目标系统的数据库敏感信息。泛微 E-cology OA 系统 JSP 版本均受此漏洞影响。

处置建议

目前，泛微官方已发布漏洞补丁，请用户及时确认是否受到漏洞影响，尽快采取修补措施。官方补丁地址如下：

https://www.weaver.com.cn/cs/securityDownload.asp

参考链接：

http://www.cnnvd.org.cn/web/bulletin/bulletinById.tag?mkid=163

河南省教育信息安全监测中心

网址：http://aqtb.ha.edu.cn

邮箱：hercert@ha.edu.cn

电话：0371-67761893、0371-67765016