河南省教育信息安全监测中心
关于正方软件教务管理系统存在越权访问漏洞的安全风险预警

2024 年 4 月 22 日

关于正方软件教务管理系统存在越权访问漏洞的安全风险预警

漏洞说明

近期监测发现杭州正方软件股份有限公司开发的教务管理系统存在高危漏洞的情况，其相关业务接口未配置认证措施，攻击者可构造恶意请求对业务接口进行越权等恶意操作，获取敏感个人信息等重要数据。

请各单位做好自查工作，迅速组织排查该系统漏洞存在情况，如发生重大网络安全事件应及时处置并报告。

漏洞编号

无

漏洞危害

高危

漏洞详情

- 访问地址

http://学校实际地址/jwglxt/xtgl/yhgl_xgBcYhxx.html?gnmkdm=N102020&doType=save

&jsdminner=xs&jsmc=%E5%AD%A6%E7%94%9F&yhm=1512180102&xm=%E6%B2%88%E6%80%A1&dzyx=&sjhm=&jgmc=0226%E6%B5%8B%E8%AF%95%E5%AD%A6%E9%99%A2&jg_id=1246E830FCD92508E063841D470A5190&autocomplete=&cbvjsxx=xygly&cbvjsxx=AA7242BB692D7C76E0538413470AE8C8&cbvjsxx=xs&sfqy=1&sykssj=&syjssj=&dlip=*

在获取正确的用户名及密码后，登录系统获取学生帐号的 cookie 信息。利用获得的 cookie 信息(保持学生帐号的登录状态),使用第三方工具进行接口访问，进行调用结果提示“保存成功”。

- 原因分析

在系统外获取到正确的帐号及密码后，利用教务系统在用户权限设计上的不完善获得教师信息导出权限。

安全建议

1. 通过采用全局权限拦截器的方式对系统接口进行严格权限控制，禁止用户访问未经授权的接口；
2. 联系供应链厂商进行修复。

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