关于对致远 OA 系统存在文件上传漏洞开展安全加固的预警通知

校属各单位：

根据上级预警通知，致远 OA 系统存在文件上传漏洞。攻击者利用该漏洞，可在未授权的情况下上传恶意文件，获取目标服务器权限。目前，漏洞细节已公开，厂商已发布版本补丁修复。

一、漏洞情况分析

近日，有安全人员披露了致远 OA 系统的高危漏洞。未经身份验证的攻击者利用该漏洞，可通过精心构造恶意脚本文件，使用 POST 方法向目标服务器上传该文件，上传后即可通过远程执行代码，实现网站后门的植入，进而控制目标服务器。目前，漏洞细节已公开，厂商已发布版本补丁修复。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

漏洞影响的产品版本包括：

致远 OA V8.0

致远 OA V7.1、V7.1SP1

致远 OA V7.0、V7.0SP1、V7.0SP2、V7.0SP3

致远 OA V6.0、V6.1SP1、V6.1SP2

致远 OA V5.x

三、漏洞处置建议

目前，致远 OA 官方已发布补丁完成漏洞修复，建议用户立即通

过官方网站安装最新补丁：

http://service.seeyon.com/patchtools/tp.html#/patchList?type=%E5%AE%89%E5%85%A8%E8%A1%A5%E4%B8%81&id=1

鉴于漏洞影响较广、危害较大，请单位务必高度重视，及时修复漏洞，消除安全隐患。

联系人：侯国平　　电话：65362000

信息技术中心

2021 年 1 月 11 日