



河南省教育信息安全监测中心

致远 OA 前台密码重置漏洞

安全风险预警



致远 OA 前台密码重置漏洞

安全风险预警

事件描述

致远 OA 是北京致远互联软件股份有限公司开发的一套办公自动化软件。

近日，致远发布安全公告，修复了一处短信验证码认证缺陷导致的任意用户密码修改漏洞，攻击者可以利用此漏洞修改任意账号的密码，进而登录系统并获取密码被修改账号的访问权限，进一步的利用后台接口可以导致远程代码执行。

漏洞编号

暂无

漏洞危害

高危

影响范围

致远 OA=V5

致远 OA=G6

致远 OA=V8.1SP2

致远 OA=V8.2

安全建议

1、官方已修复该漏洞，建议按照官方修复步骤修复此漏洞。

参考连接：

<https://service.seeyon.com/patchtools/tp.html#/patchList?type=%E5%AE%89>

%E5%85%A8%E8%A1%A5%E4%B8%81&id=171

2、临时防护方案：

- 1) 加强系统和网络的访问控制，修改防火墙策略，不将非必要服务暴露于公网；
- 2) 在公网部署的系统，通过 WAF 限制外网对“/seeyon/personalBind.do”，
“/seeyon/individualManager.do?method=resetPassword” 等路径的访问；
- 3) 定期对服务器上的网站后门文件进行及时查杀。

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