河南省教育信息安全监测中心

致远 OA M1 移动端存在远程代码执行漏洞安全风险预警

2023 年 09 月 08 日

致远 OA M1 移动端存在远程代码执行漏洞安全风险预警

事件描述

致远 OA M1 移动端是由北京致远互联软件股份有限公司开发的一款可以实现在任何时间、任何地点、任何环境都能让用户“轻松、便捷、高效”完成工作的协同办公管理软件。同时，还可以实现 PC 端、移动端、web 端，三端合一，无缝实时覆盖，实现管理无中断

近日发现，致远 OA M1 移动端存在 RCE 漏洞。由于致远 OA M1 Server userTokenService 接口存在反序列化漏洞，且未对该接口的调用请求采用严格的身份验证和安全过滤机制，导致未经授权的攻击者可以构造恶意的序列化数据以远程执行任意命令，最终获取到服务器权限。

漏洞编号

暂无

漏洞危害

高危

影响范围

致远互联-M1 移动端

安全建议

1、官方已发布相关安全修复补丁，建议用户咨询售后技术人员获取安全修复方案。

https://support.seeyon.com/

2、可使用 Web 防火墙等安全设备实时监控后台访问行为，对访问中存在调用 userTokenService 接口的未授权请求，进行强身份验证并且过滤不安全字符串。

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