iMC&U-Center不涉及漏洞 蓝凌 OA 远程代码执行漏洞

PLAT 付帅文 2021-04-18 发表

漏洞相关信息

漏洞编号： 无
漏洞名称： 蓝凌 OA 远程代码执行漏洞
产品型号及版本： iMC_1.0系列产品，U-Center1.0系列产品

漏洞描述

漏洞原理：蓝凌 OA 的 dataxml.jsp 文件中指定了若干数据处理方法，当指定 s_bean参数值为 sysFormulaVaildate 时，可以通过 script 参数提交一段 java 代码，服务器收到请求后将在后台执行这段代码，因此攻击者可以通过构造请求包尝试在服务器写入 webshell。 漏洞特征：1）请求 URL 特征：url：/sys/common/dataxml.jsp；2）请求参数特征：s_bean=sysFormulaVaildate,script=exp 处置/应对措施：1)排查当前版本的蓝凌 OA dataxml.jsp 文件中是否允许调用sysFormulaVaildate 组件；2) 在安全设备中增加特征监控策略： 将 POST 请求/ekp/sys/common/dataxml.jsp 且参数 s_bean 为 sysFormulaValidate 的请求进行拦截或告警。

漏洞解决方案

iMC&U-Center1.0系列皆不涉及该漏洞，可参考漏洞报告进行漏洞修复，不影响iMC&U-Center1.0功能。