iMC&U-Center不涉及Apache Tapestry远程代码执行漏洞

PLAT Ucenter 栗鹏 2021-04-19 发表

漏洞相关信息

漏洞编号： 无

漏洞名称： Apache Tapestry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

攻击者可以通过请求包含HMAC秘钥的URL http://localhost:8080/assets/something/services/AppModule.class来下载文件AppModule.class。CVE-2019-0195的修复使用了黑名单过滤，其检查URL是否以“.class”、“.properties”或“.xml”结尾，但这种黑名单过滤可以通过在URL结尾添加“/”来绕过。 当 http://localhost:8080/assets/something/services/AppModule.class/在黑名单检查后，斜线被剥离，AppModule.class文件被加载到响应中。这个类通常包含用于对序列化的Java对象进行签名的HMAC秘钥，在知道该密钥的情况下，攻击者就可以签署Java小工具链（例如ysoserial的CommonsBeanUtils1），最终导致远程代代码执行。

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。