iMC&U-Center是否涉及漏洞CVE-2020-9484

PLAT 汤祺 2021-03-17 发表

漏洞相关信息

漏洞编号： CVE-2020-9484
漏洞名称： Apache Tomcat session持久化远程代码执行漏洞
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

【漏洞详情】
Apache Tomcat 是一个开放源代码、运行servlet和JSP Web应用软件的基于Java的Web应用软件容器。当Tomcat使用了自带session同步功能时，使用不安全的配置（没有使用EncryptInterceptor）会存在反序列化漏洞，攻击者通过精心构造的数据包， 可以对使用了自带session同步功能的Tomcat服务器进行攻击。
成功利用此漏洞需要同时满足以下4个条件:
1.攻击者能够控制服务器上文件的内容和文件名称
2.服务器PersistenceManager配置中使用了FileStore
3.PersistenceManager中的sessionAttributeValueClassNameFilter被配置为“null”，或者过滤器不够严格，导致允许攻击者提供反序列化数据的对象
4.攻击者知道使用的FileStore存储位置到攻击者可控文件的相对路径
【漏洞等级】
中危
【受影响版本】

- iMC_PLAT_0705P07以前版本

漏洞解决方案

iMC：升级平台至E0705P07及以上版本进行漏洞修复，组件版本需查看版本说明书中平台版本的适配关系确认是否需要同步升级
U-Center：升级平台版本至E0705P07进行漏洞修复，U-Center运维组件版本需查看版本说明书中平台版本的适配关系确认是否需要同步升级