

知 iMC&U-Center1.0是否涉及Spring 框架远程代码执行高危漏洞

PLAT

Ucenter

贾海韵

2022-04-08 发表

漏洞相关信息

漏洞编号: CVE-2022-22965

漏洞名称: Spring 框架远程代码执行高危漏洞

产品型号及版本: iMC&U-Center1.0

漏洞描述

3月30日, Spring框架曝出RCE 0day漏洞。已经证实由于 `SerializationUtils#deserialize` 基于 Java 的序列化机制, 可导致远程代码执行 (RCE), 使用JDK9及以上版本皆有可能受到影响。

漏洞详情参考链接: <https://www.freebuf.com/vuls/326627.html>

目前, 漏洞利用细节已大范围公开, Spring官方已发布补丁修复该漏洞。

目前已知, 触发该漏洞需要满足两个基本条件:

1. 使用JDK9及以上版本的Spring MVC框架;
2. Spring 框架以及衍生的框架spring-beans-*.jar 文件或者存在CachedIntrospectionResults.class.

漏洞解决方案

包含UEM功能的BSM组件涉及该漏洞，不包含UEM功能的不涉及。计划5月份出新版本（预计0711版本）解决。

目前临时解决方案：拨打400，反馈现场的..\iMC\client\uembin\uem.jar文件，修改后返回现场替换，最后重启uem进程。

除此之外，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。

