

知 U-Center2.0是否涉及Spring 框架远程代码执行高危漏洞

U-Center 2.0 贾海韵 2022-04-06 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: U-Center2.0

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:

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

漏洞解决方案

U-Center2.0 E060X分支不涉及该漏洞，可参考漏洞报告进行漏洞修复，不影响 U-Center2.0功能。

U-Center2.0 E070X 分支涉及，预计4月底的0707版本解决。

