Spring4Shell 的漏洞说明

漏洞说明

spring官网发布了关于Spring4Shell的安全漏洞，具体可查看 Spring Framework RCE, Early Announcement。

Spring4Shell 漏洞对于smartbi影响性说明

根据 Spring Framework RCE, Early Announcement 报告分析：

1、此漏洞为 Spring 在处理表单上传数据对象时，没有正确的过滤不安全数据，导致可以触发到 Tomcat 的安全漏洞。从而实现 Shell 的漏洞入口，并可在服务器上执行命令

2、漏洞需要在JDK 9+，并且使用表单上传数据时才能生效。而在 Smartbi 中前后端交互时使用的为 JSON 格式，在 JSON 格式的传输方式下并不会触发此漏洞

3、Spring针对此漏洞发布了修复版本 5.3.18 and 5.2.20，Tomcat 10.0.20, 9.0.62, and 8.5.78 均修复了此漏洞

4、产品本身带的 Spring 版本是 4.2.29，针对 4.x 版本并无官方的修复版本，而产品跨大版本升级 Spring 框架是需要较长时间测试验证的

5、目前产品应当是不受此安全漏洞影响，客户如果有担忧则建议考虑升级 Tomcat 版本：至10.0.20、9.0.62、8.5.78