H3C SecPath GAP2000系列安全隔离与信息交换系统是否涉及Spring框架远程代码执行高危

漏洞相关 卢鹏 2022-04-08 发表

漏洞相关信息

漏洞编号： 暂无

漏洞名称： Spring框架远程代码执行高危

产品型号及版本： H3C SecPath GAP2000系列安全隔离与信息交换系统

漏洞描述

I、执行“java -version”命令查看运行JDK版本。如果版本号小于等于8，则不受漏洞影响。

II、Spring 框架使用情况排查

一.如果业务系统项目以war包形式部署，按照如下步骤进行判断。

1）解压war包：将war文件的后缀修改成.zip，解压zip文件。

2）在解压缩目录下搜索是否存在spring-beans-*.jar格式的jar文件（例如spring-beans-5.3.16.jar）,如存在则说明业务系统使用了Spring框架进行开发。

3）如果spring-beans-*.jar文件不存在，则在解压缩目录下搜索CachedIntrospectionResults.class文件是否存在，如存在则说明业务系统使用了Spring框架进行开发。

二、如果业务系统项目以jar包形式直接独立运行，按照如下的步骤进行判断。

1）�! 压jar ：将jar包文件的后缀修改成.zip,解压zip文件。

2）在解压缩目录下搜索是否存在spring-beans-*.jar格式的jar文件（例如spring-beans-5.3.16.jar）,如存在则说明业务系统使用了Spring框架进行开发。

3）如果spring-beans-*.jar文件不存在，则在解压缩目录下搜索CachedIntrospectionResults.class文件是否存在，如存在则说明业务系统使用了Spring框架进行开发。

三、综合判断

在完成以上两个步骤排查后，同时满足以下两个条件可确定受此漏洞影响：

1）JDK版本号在9及以上的；

2）使用了Spring框架或衍生框架。

漏洞解决方案

不涉及