Fortify扫描问题

项目	安全事件来源	详细事件	修复方案	工作项状态	实际开始时间	实际完成时间	执行人	备注
shine-soa-dfa-boot	Cookie Security: Overly Broad Path (Security Features, Semantic) 可通过相同域中的其他应用程序访问路径范围过大的cookie。（2个）	Recommendations: 确保将cookie路径设置为具有尽可能高的限制性。 例2：以下代码显示如何针对“说明”部分中的示例将cookie路径设置为"/MyForum" Cookie cookie = new Cookie("sessionID", sessionID); cookie.setPath("/MyForum"');		完成				
common-dfa-boot	Weak Encryption: Insecure Mode of Operation (Security	Recommendations: 加密大于块的数据时，避免使用ECB 操	去除此Utils，添加SM4Utils替代	完成				

	Features, Semantic) DesUtils.java中的西数encrypt0在第77行上将密码加密算法用于不安全的操作模式。（7个）	作模式。CBC 模式更好，因为它不会对相同的明文块生成相同的密文块。然而，CBC模式效率较低，并且在和 SSL 一起使用时会造成严重风险。[1] 请改用 CCM (Counter with CBC-MAC) 模式，或者如果更注重性能，则使用 GCM （Galois/Counter模式）模式（如可用）。						
web-dfa-boot	Denial of Service: Regular Expression (Input Validation and Representation, Data Flow) 不受信数据被传递	Recommendations: 请不要将不可信赖的数据用作正则表达式。	使用逻辑替换正则表达式	完成				

	至应用程序并作为正则表达式使用。这会导致线程过度使用 CPU 资源。							
	assword Management: Hardcoded Password (Security Features, Structural) Hardcoded password 可能会危及系统安全性，并且无法轻易修正出现的安全问题。（1 个）	Recommendations: 请勿对加密密钥进行硬编码，而应对加密密钥加以模糊化，并在外部资源文件中进行管理。如果在系统中采用明文的形式存储加密密钥，任何有足够权限的人即可读取加密密钥，还可能误用这些密码。	去除关键字	完成				
rpc-dfa-boot	Weak Encryption: Insecure Mode of Operation (Security Features,	Recommendations: 加密大于块的数据时，避免使用 ECB 操作模式。CBC 模式更好，	去除此 Utils，添加 SM4Utils 替代	完成				

	Semantic) DesUtils.java中的西数encrypt0在第77行上将密码加密算法用于不安全的操作模式。（6个）	因为它不会对相同的明文块生成相同的密文块。然而，CBC模式效率较低，并且在和SSL 一起使用时会造成严重风险。[1] 请改用CCM (Counter with CBC-MAC) 模式，或者如果更注重性能，则使用GCM （Galois/Counter模式）模式（如可用）。						
jdbc-dfa-boot	Password Management: Hardcoded Password (Security Features, Structural) Hardcoded passwor	Recommendations: 请勿对加密密钥进行硬编码，而应对加密密钥加以模糊化，并在外部资源文件中进行管理。如果在系统中采用明文	去除关键字	完成				

	d 可能会危及系统安全性，并且无法轻易修正出现的安全问题。（1个）	的形式存储加密密钥，任何有足够权限的人即可读取加密密钥，还可能误用这些密码。						
runtime-dfa-boot	Key Management: Hardcoded Encryption Key (Security Features, Structural) 硬编码加密密钥可能会削弱安全性，旦出现安全问题将无法轻易修正。（1个）	Recommendations: 请勿对加密密钥进行硬编码，而应对加密密钥加以模糊化，并在外部资源文件中进行管理。如果在系统中采用明文的形式存储加密密钥，任何有足够权限的人即可读取加密密钥，还可能误用这些密码。	去除关键字	完成				
	Password Management: Hardcoded Password (Security	Recommendations: 请勿对加密密钥进行硬编码，而应对加密密钥加以模糊化，并	去除关键字	完成				

	Features, Structural) Hardcoded password 可能会危及系统安全性，并且无法轻易修正出现的安全问题。	在外部资源文件中进行管理。如果在系统中采用明文的形式存储加密密钥，任何有足够权限的人即可读取加密密钥，还可能误用这些密码。						
DFA-RPC-ALL	无			无需变动				
DFA-RPC-SDK	Weak Encryption: Insecure Mode of Operation (Security Features, Semantic) DesUtils.java中的西数encrypt0在第77行上将密码加密算法用于不安全的操作模式。（6个）	Recommendations: 加密大于块的数据时，避免使用 ECB 操作模式。CBC 模式更好，因为它不会对相同的明文块生成相同的密文块。然而，CBC模式效率较低，并且在和 SSL 一起使用时会造成严重风险。[1] 请改用 CCM	去除此Utils，添加SM4Utils替代	完成				

		(Counter with CBC-MAC) 模式，或者如果更注重性能，则使用 GCM （Galois/Counter 模式）模式（如可用）。						
中债登 SDK	无							

AppScan扫描

使用unittest扫描不准确，建议使用BMS或者UAS扫描后识别是DFA-Boot的问题进行调整。

Jar包漏洞概述

DFA-Boot依赖的jar包有部分依赖暂未修复，具体清单如下：

项目	包	版本	建议版本	工作项进度	备注
rpc-dfa-boot	org.jboss.resteasy:resteasy-client	3.6.3.Final	4.5.7.Final	未开始	版本跨度太大，且依赖是由sofa-rpc引进，需要进一步分析
	org.jboss.resteasy:resteasy-jaxrs	3.6.3.Final	4.5.7.Final	未开始	版本跨度太大，且依赖是由sofa-rpc引进，需要进一步分析

无法修复，详情查看：

https://github.com/sofastack/sofa-rpc/pull/1072

sofa-rpc的commiter

OrezzerO commented on 14 Sep 2021

update resteasy version is dangerous for RPC，I will close it

故暂时无法升级。

小结

1. 安全漏洞问题均解决
2. jar包漏洞遗留两个问题未解决：

org.jboss.resteasy:resteasy-client

org.jboss.resteasy:resteasy-jaxrs