CMStore

应用检测报告

创建人员：王兵

报告编号：BG-20231013-8736

报告类型：应用检测报告

创建时间：2024-06-11 12:43:37

声明

本机构保证检测的客观性、科学性和公正性，本报告仅对测试样品版本、测试环境和测试数据当时的状态有效、由于系统或软件发生变更而涉及到的系统构成组件（或子系统）都应重新进行评测，本报告不再适用。

本报告仅对所检测对象给出的结果，不代表未经检测的对象或功能符合要求；也不能作为系统或软件内部部署的相关系统构成组件（或产品）的结论；也并非是系统或软件运行健康状态的表示。

本报告的有效性建立在被测单位提供相关证据的真实性基础之上。

在任何情况下，若需引用本报告中的测试结果或结论都应该保持其原有的意义，不得对相关内容擅自进行增加、修改、删减、伪造或掩盖事实。

本报告涂改无效。

2023 年 09 月 15 日

1 概览

1.1 基本信息

表 1-1 应用检测基本信息表

应用名称	CMStore
公司类型	直属单位
所属公司	信息技术中心（公司）
所属部门	平台能力中心
所属工程	系统：CMStore
负责人	李善航（所属公司：信息技术中心（公司），账户名：lish_a，联系方式：15274942884）
下载源校验	成功：32，失败：0
应用创建时间	2023-10-13 09:28:15
扫描开始时间	2024-06-11 12:40:47
扫描结束时间	2024-06-11 12:42:04
扫描耗时	1 分 17 秒
扫描方式	上传特征文件
扫描路径	不涉及

1.2 统计信息

本次对“CMStore”进行了开源威胁检测，检测统计信息具体如下：

- 共发现 **32 个开源组件**：其中**超危组件 1 个**，**高危组件 3 个**，中危组件 3 个，低危组件 0 个，安全组件 25 个；通过对组件的名单类型进行识别得出：白名单组件 20 个，**黑名单组件 0 个**，名单外组件 12 个；
- 共发现 **18 个漏洞**：其中**超危漏洞 1 个**，**高危漏洞 5 个**，中危 11 个，低危 1 个；
- 共发现许**可证类型有 12 条**：其中高风险许可证 0 条，中风险许可证 4 条，低风险许可证 5 条；

为了项目及应用安全，请相关人员及时修复风险。

1.2.1 组件风险统计

表 1-2 组件风险等级统计表

组件风险级别	组件数量
超危	1
高危	3
中危	3
低危	0
安全	25
未知	0
总计	32

表 1-3 组件名单类型统计表

组件名单类型	组件数量
黑名单	0
灰名单	0
名单外	12
白名单	20

1.2.2 漏洞风险统计

表 1-4 漏洞风险等级统计表

漏洞风险级别	漏洞数量
超危	1
高危	5
中危	11
低危	1
未知	0
总计	18

1.2.3 许可证风险统计

表 1-5 许可证风险等级统计表

许可证风险级别	组件数量
高风险	0
中风险	4
低风险	5
未知	3
总计	12

2 组件

2.1 组件风险列表

表 2-1 组件风险列表

组件名称	版本	所属语言	风险等级	许可证	名单类型	引入来源
spring-core	4.3.29.RELEASE	Java	超危	Apache-2.0	名单外	
jackson-databind	2.12.6	Java	高危	Apache-2.0	名单外	
gson	2.8.6	Java	高危	Apache-2.0	名单外	
guava	18.0	Java	高危	Apache-2.0	名单外	
bcprov-jdk15on	1.67	Java	中危	未声明	名单外	
httpclient	4.4.1	Java	中危	Apache-1.0,Apache-2.0	名单外	

poi	3.17	Java	中危	Apache-2.0	名单外	
jackson-annotations	2.12.6	Java	安全	Apache-2.0	白名单	
httpmime	4.4.1	Java	安全	Apache-1.0,Apache-2.0	白名单	
jaxb-api	2.3.1	Java	安全	CDDL-1.1,GPL-2.0-with-classpath-exception	白名单	
javax.activation-api	1.2.0	Java	安全	CDDL-1.0	白名单	
hamcrest-core	1.3	Java	安全	BSD-3-Clause	白名单	
org.jacoco.agent	0.8.5	Java	安全	Clips,EPL-2.0	名单外	
jdom2	2.0.6.1	Java	安全	TCL	白名单	
ncoss-java-sdk	2.0.2-RELEASE	Java	安全	未声明	名单外	
commons-logging	1.2	Java	安全	Apache-1.0,Apache-2.0	白名单	
opentracing-api	0.33.0	Java	安全	Apache-1.0,Apache-2.0	白名单	
httpcore	4.4.1	Java	安全	Apache-1.0,Apache-2.0	白名单	
slf4j-api	1.7.30	Java	安全	MIT	白名单	
commons-collections4	4.1	Java	安全	Apache-1.0,Apache-2.0	白名单	
fastjson	1.2.83	Java	安全	Apache-2.0	白名单	
opentracing-noop	0.33.0	Java	安全	Apache-1.0,Apache-2.0	白名单	
opentracing-util	0.33.0	Java	安全	Apache-1.0,Apache-2.0	白名单	
slf4j-simple	1.7.30	Java	安全	MIT	名单外	
jettison	1.5.4	Java	安全	Apache-2.0	白名单	
ini4j	0.5.4	Java	安全	Apache-2.0	白名单	
commons-codec	1.9	Java	安全	Apache-1.0,Apache-2.0	白名单	
jackson-core	2.12.6	Java	安全	Apache-2.0	名单外	
jackson-mapper-asl	0.9.6	Java	安全	Apache-2.0	名单外	

junit	4.13.2	Java	安全	Clips,EPL-1.0	白名单	
jackson-core-asl	1.9.13	Java	安全	Apache-2.0	白名单	
lombok	1.18.12	Java	安全	MIT	白名单	

2.2 组件风险详情

2.2.1 spring-core

基本信息

风险等级	超危
当前版本	4.3.29.RELEASE
所属语言	Java
发布厂商	org.springframework
名单类型	名单外
推荐版本	6.0.8
最新版本	6.1.6
是否开源	开源
下载源校验	成功
发布日期	2020-09-15
许可证	Apache-2.0
引入方式	
漏洞分布	超危 1、高危 0、中危 5、低危 0

引入来源

漏洞列表（6）

漏洞名称	Spring Framework 代码注入漏洞
风险等级	超危
漏洞类型	代码注入
发布时间	2022-03-30
CVE 编号	CVE-2022-22965
CNNVD 编号	CNNVD-202203-2514
CNVD 编号	
CWE 编号	CWE-94
利用难度	中
漏洞描述	lux 是一款加密货币。JDK 是 Sun 微系统针对 Java 开发人员发布的免费软件开发工具包（SDK，Software development kit）。 Spring Framework 存在代码注入漏洞，该漏洞源于 JDK 9+ 上的数据绑定的 RCE。以下产品和版本受到影响：5.3.0 至 5.3.17、5.2.0 至 5.2.19、较旧的和不受支持的版本也会受到影响。
修复建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://tanzu.vmware.com/security/cve-2022-22965

漏洞名称	Vmware Spring Framework 安全特征问题漏洞
风险等级	中危
漏洞类型	安全特征问题
发布时间	2022-04-13
CVE 编号	CVE-2022-22968
CNNVD 编号	CNNVD-202204-3302
CNVD 编号	
CWE 编号	CWE-178
利用难度	中
漏洞描述	Vmware Spring Framework 是美国威睿（Vmware）公司的一套开源的 Java、JavaEE 应用程序框架。该框架可帮助开发人员构建高质量的应用。 Vmware Spring Framework 存在安全特征问题漏洞，该漏洞源于 DataBinder 上 disallowedFields 的模式是区分大小写的，这意味着字段没有得到有效保护，除非该字段的第一个字符同时以大写和小写字母列出，包括属性路径中所有嵌套字段的第一个字符的大写和小写字母。远程攻击者利用该漏洞可以绕过实施的安全限制。
修复建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://tanzu.vmware.com/security/cve-2022-22968

漏洞名称	Spring Framework 输入验证错误漏洞
风险等级	中危
漏洞类型	输入验证错误
发布时间	2022-05-11
CVE 编号	CVE-2022-22970
CNNVD 编号	CNNVD-202205-2988
CNVD 编号	
CWE 编号	CWE-770
利用难度	低
漏洞描述	Spring Framework 是美国 Spring 团队的一套开源的 Java、JavaEE 应用程序框架。该框架可帮助开发人员构建高质量的应用。 Spring Framework 存在输入验证错误漏洞，攻击者利用该漏洞可通过将数据绑定到 MultipartFile 导致 Spring Framework 致命的错误，从而触发拒绝服务。
修复建议	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法： https://spring.io/projects/spring-framework

漏洞名称	Spring Framework 输入验证错误漏洞
风险等级	中危
漏洞类型	输入验证错误
发布时间	2022-05-11
CVE 编号	CVE-2022-22971
CNNVD 编号	CNNVD-202205-2980
CNVD 编号	
CWE 编号	CWE-770
利用难度	低

漏洞描述	Spring Framework 是美国 Spring 团队的一套开源的 Java、JavaEE 应用程序框架。该框架可帮助开发人员构建高质量的应用。 Spring Framework 存在输入验证错误漏洞。攻击者利用该漏洞通过 WebSocket 上的 STOMP 导致 Spring Framework 的致命错误，以触发拒绝服务。
修复建议	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://spring.io/projects/spring-framework

漏洞名称	CVE-2023-20861
风险等级	中危
漏洞类型	NVD-CWE-noinfo
发布时间	2023-03-23
CVE 编号	CVE-2023-20861
CNNVD 编号	
CNVD 编号	
CWE 编号	NVD-CWE-noinfo
利用难度	低
漏洞描述	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.
修复建议	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

漏洞名称	CVE-2023-20863
风险等级	中危
漏洞类型	CWE-917
发布时间	2023-04-13
CVE 编号	CVE-2023-20863
CNNVD 编号	
CNVD 编号	
CWE 编号	CWE-917
利用难度	低
漏洞描述	In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.
修复建议	In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

2.2.2 jackson-databind

基本信息

风险等级	高危
当前版本	2.12.6
所属语言	Java
发布厂商	com.fasterxml.jackson.core
名单类型	名单外
推荐版本	2.4.6.1
最新版本	2.17.1
是否开源	开源
下载源校验	成功
发布日期	2021-12-15
许可证	Apache-2.0
引入方式	
漏洞分布	超危 0、高危 3、中危 0、低危 0

引入来源

漏洞列表（3）

漏洞名称	FasterXML jackson-databind 缓冲区错误漏洞
风险等级	高危
漏洞类型	缓冲区错误
发布时间	2022-03-11
CVE 编号	CVE-2020-36518
CNNVD 编号	CNNVD-202203-1165
CNVD 编号	
CWE 编号	CWE-787
利用难度	中
漏洞描述	FasterXML jackson-databind 是一个基于 JAVA 可以将 XML 和 JSON 等数据格式与 JAVA 对象进行转换的库。Jackson 可以轻松的将 Java 对象转换成 json 对象和 xml 文档，同样也可以将 json、xml 转换成 Java 对象。 FasterXML jackson-databind 2.13.0 之前版本中存在安全漏洞，该漏洞源于软件中存在 Java 的栈溢出异常，攻击者可以通过大量嵌套对象利用该漏洞实现拒绝服务攻击。
修复建议	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法： https://github.com/FasterXML/jackson-databind/issues/2816

漏洞名称	CVE-2022-42003
风险等级	高危
漏洞类型	CWE-502
发布时间	2022-10-02
CVE 编号	CVE-2022-42003
CNNVD 编号	
CNVD 编号	
CWE 编号	CWE-502
利用难度	中

漏洞描述	In FasterXML jackson-databind before versions 2.13.4.1 and 2.12.17.1, resource exhaustion can occur because of a lack of a check in primitive value deserializers to avoid deep wrapper array nesting, when the UNWRAP_SINGLE_VALUE_ARRAYS feature is enabled.
修复建议	In FasterXML jackson-databind before versions 2.13.4.1 and 2.12.17.1, resource exhaustion can occur because of a lack of a check in primitive value deserializers to avoid deep wrapper array nesting, when the UNWRAP_SINGLE_VALUE_ARRAYS feature is enabled.

漏洞名称	CVE-2022-42004
风险等级	高危
漏洞类型	CWE-502
发布时间	2022-10-02
CVE 编号	CVE-2022-42004
CNNVD 编号	
CNVD 编号	
CWE 编号	CWE-502
利用难度	中
漏洞描述	In FasterXML jackson-databind before 2.13.4, resource exhaustion can occur because of a lack of a check in BeanDeserializer._deserializeFromArray to prevent use of deeply nested arrays. An application is vulnerable only with certain customized choices for deserialization.
修复建议	In FasterXML jackson-databind before 2.13.4, resource exhaustion can occur because of a lack of a check in BeanDeserializer._deserializeFromArray to prevent use of deeply nested arrays. An application is vulnerable only with certain customized choices for deserialization.

2.2.3 gson

基本信息

风险等级	高危
当前版本	2.8.6
所属语言	Java
发布厂商	com.google.code.gson
名单类型	名单外
推荐版本	2.8.9
最新版本	2.10.1
是否开源	开源
下载源校验	成功
发布日期	2019-10-05
许可证	Apache-2.0
引入方式	
漏洞分布	超危 0、高危 1、中危 0、低危 0

引入来源

漏洞列表（1）

漏洞名称	gson 代码问题漏洞
风险等级	高危
漏洞类型	代码问题
发布时间	2022-05-01
CVE 编号	CVE-2022-25647
CNNVD 编号	CNNVD-202205-1791
CNVD 编号	
CWE 编号	CWE-502
利用难度	中
漏洞描述	gson 是一个 Java 库，可用于将 Java 对象转换为其 JSON 表示形式。com.google.code.gson:gson 2.8.9 之前版本存在安全漏洞，该漏洞源于 writeReplace()方法反序列化不受信任的数据，可导致 DoS 攻击。
修复建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/google/gson/pull/1991/files

2.2.4 guava

基本信息

风险等级	高危
当前版本	18.0
所属语言	Java
发布厂商	com.google.guava
名单类型	名单外
推荐版本	32.0.0-android
最新版本	33.2.0-jre
是否开源	开源
下载源校验	成功
发布日期	2014-08-26
许可证	Apache-2.0
引入方式	
漏洞分布	超危 0、高危 1、中危 1、低危 1

引入来源

漏洞列表（3）

漏洞名称	CVE-2023-2976
风险等级	高危
漏洞类型	CWE-552
发布时间	2023-06-14
CVE 编号	CVE-2023-2976
CNNVD 编号	

CNVD 编号	
CWE 编号	CWE-552
利用难度	低
漏洞描述	Use of Java's default temporary directory for file creation in `FileBackedOutputStream` in Google Guava versions 1.0 to 31.1 on Unix systems and Android Ice Cream Sandwich allows other users and apps on the machine with access to the default Java temporary directory to be able to access the files created by the class. Even though the security vulnerability is fixed in version 32.0.0, we recommend using version 32.0.1 as version 32.0.0 breaks some functionality under Windows.
修复建议	Use of Java's default temporary directory for file creation in `FileBackedOutputStream` in Google Guava versions 1.0 to 31.1 on Unix systems and Android Ice Cream Sandwich allows other users and apps on the machine with access to the default Java temporary directory to be able to access the files created by the class. Even though the security vulnerability is fixed in version 32.0.0, we recommend using version 32.0.1 as version 32.0.0 breaks some functionality under Windows.

漏洞名称	Google Guava 代码问题漏洞
风险等级	中危
漏洞类型	代码问题
发布时间	2018-04-27
CVE 编号	CVE-2018-10237
CNNVD 编号	CNNVD-201804-1461
CNVD 编号	CNVD-2018-10064
CWE 编号	CWE-770
利用难度	低
漏洞描述	Google Guava 是美国谷歌（Google）公司的一款包括图形库、函数类型、I/O 和字符串处理等的 Java 核心库。 Google Guava 11.0 版本至 24.1.1 版本（不包括 24.1.1 版本）中存在代码问题漏洞。该漏洞源于网络系统或产品的代码开发过程中存在设计或实现不当的问题。
修复建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://groups.google.com/forum/#!topic/guava-announce/xqWALw4W1vs/discussion

漏洞名称	Google Guava 访问控制错误漏洞

风险等级	低危
漏洞类型	访问控制错误
发布时间	2020-12-10
CVE 编号	CVE-2020-8908
CNNVD 编号	CNNVD-202012-827
CNVD 编号	CNVD-2021-31252
CWE 编号	CWE-732
利用难度	低
漏洞描述	Google Guava 是美国谷歌（Google）公司的一款包括图形库、函数类型、I/O 和字符串处理等的 Java 核心库。 Google Guava 30.0 版本之前存在访问控制错误漏洞，该漏洞源于 Guava 存在一个临时目录创建漏洞，允许访问机器的攻击者可利用该漏洞潜在地访问由 Guava com.google.common.io. Files. createTempDir() 创建的临时目录中的数据。攻击者可以利用该漏洞访问特殊目录。
修复建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://github.com/google/guava/issues/4011

2.2.5 bcprov-jdk15on

基本信息

风险等级	中危
当前版本	1.67
所属语言	Java
发布厂商	org.bouncycastle
名单类型	名单外
推荐版本	1.68
最新版本	1.70
是否开源	开源
下载源校验	成功
发布日期	2020-11-01
许可证	未声明
引入方式	
漏洞分布	超危 0、高危 0、中危 2、低危 0

引入来源

漏洞列表（2）

漏洞名称	CVE-2023-33201
风险等级	中危
漏洞类型	CWE-295
发布时间	2023-07-05
CVE 编号	CVE-2023-33201
CNNVD 编号	
CNVD 编号	
CWE 编号	CWE-295
利用难度	中

漏洞描述	Bouncy Castle For Java before 1.74 is affected by an LDAP injection vulnerability. The vulnerability only affects applications that use an LDAP CertStore from Bouncy Castle to validate X.509 certificates. During the certificate validation process, Bouncy Castle inserts the certificate's Subject Name into an LDAP search filter without any escaping, which leads to an LDAP injection vulnerability.
修复建议	Bouncy Castle For Java before 1.74 is affected by an LDAP injection vulnerability. The vulnerability only affects applications that use an LDAP CertStore from Bouncy Castle to validate X.509 certificates. During the certificate validation process, Bouncy Castle inserts the certificate's Subject Name into an LDAP search filter without any escaping, which leads to an LDAP injection vulnerability.

漏洞名称	CVE-2023-33202
风险等级	中危
漏洞类型	CWE-400
发布时间	2023-11-23
CVE 编号	CVE-2023-33202
CNNVD 编号	
CNVD 编号	
CWE 编号	CWE-400
利用难度	低
漏洞描述	Bouncy Castle for Java before 1.73 contains a potential Denial of Service (DoS) issue within the Bouncy Castle org.bouncycastle.openssl.PEMParser class. This class parses OpenSSL PEM encoded streams containing X.509 certificates, PKCS8 encoded keys, and PKCS7 objects. Parsing a file that has crafted ASN.1 data through the PEMParser causes an OutOfMemoryError, which can enable a denial of service attack. (For users of the FIPS Java API: BC-FJA 1.0.2.3 and earlier are affected; BC-FJA 1.0.2.4 is fixed.)
修复建议	Bouncy Castle for Java before 1.73 contains a potential Denial of Service (DoS) issue within the Bouncy Castle org.bouncycastle.openssl.PEMParser class. This class parses OpenSSL PEM encoded streams containing X.509 certificates, PKCS8 encoded keys, and PKCS7 objects. Parsing a file that has crafted ASN.1 data through the PEMParser causes an OutOfMemoryError, which can enable a denial of service attack. (For users of the FIPS Java API: BC-FJA 1.0.2.3 and earlier are affected; BC-FJA 1.0.2.4 is fixed.)

2.2.6 httpclient

基本信息

风险等级	中危

当前版本	4.4.1
所属语言	Java
发布厂商	org.apache.httpcomponents
名单类型	名单外
推荐版本	4.5.13
最新版本	4.5.14
是否开源	开源
下载源校验	成功
发布日期	2015-03-24
许可证	Apache-1.0,Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 1、低危 0

引入来源

漏洞列表（1）

漏洞名称	Apache HttpClient 安全漏洞
风险等级	中危
漏洞类型	其他
发布时间	2020-10-08
CVE 编号	CVE-2020-13956
CNNVD 编号	CNNVD-202010-372
CNVD 编号	CNVD-2021-24248
CWE 编号	NVD-CWE-noinfo
利用难度	中
漏洞描述	HttpClient 是美国阿帕奇（Apache）基金会的一个 Java 编写的访问 HTTP 资源的客户端程序。该程序用于使用 HTTP 协议访问网络资源。Apache HttpClient java.net.URI Authority Component 存在安全漏洞，该漏洞允许攻击者访问敏感数据。
修复建议	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.apache.org/

2.2.7 poi

基本信息

风险等级	中危
当前版本	3.17
所属语言	Java
发布厂商	org.apache.poi
名单类型	名单外
推荐版本	3.0-FINAL
最新版本	5.2.5
是否开源	开源
下载源校验	成功
发布日期	2017-09-09
许可证	Apache-2.0

引入方式	
漏洞分布	超危 0、高危 0、中危 2、低危 0

引入来源

漏洞列表（2）

漏洞名称	Apache POI 代码问题漏洞
风险等级	中危
漏洞类型	代码问题
发布时间	2019-10-23
CVE 编号	CVE-2019-12415
CNNVD 编号	CNNVD-201910-1431
CNVD 编号	CNVD-2019-41291
CWE 编号	CWE-611
利用难度	低
漏洞描述	Apache POI 是美国阿帕奇（Apache）基金会的一个开源函数库，它提供 API 给 Java 程序可对 Microsoft Office 格式档案进行读和写。 Apache POI 4.1.0 及之前版本中存在代码问题漏洞。攻击者可借助特制的文档利用该漏洞读取本地文件系统中或网络资源中的文件。
修复建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://lists.apache.org/thread.html/13a54b6a03369cfb418a699180ffb83bd727320b6ddfec198b9b728e@<announce.apache.org>

漏洞名称	Apache POI 资源管理错误漏洞
风险等级	中危
漏洞类型	资源管理错误
发布时间	2022-03-04
CVE 编号	CVE-2022-26336
CNNVD 编号	CNNVD-202203-460
CNVD 编号	CNVD-2022-25193
CWE 编号	CWE-20
利用难度	低
漏洞描述	Apache POI 是美国阿帕奇（Apache）基金会的一个开源函数库，它提供 API 给 Java 程序可对 Microsoft Office 格式档案进行读和写。 Apache POI 中存在资源管理错误漏洞，该漏洞源于产品在处理文件时未能有效判断内存边界。攻击者可通过精心制作的文件可能会导致内存不足。以下产品及版本受到影响：Apache poi-scratchpad 5.2.0 版本及之前版本。
修复建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://lists.apache.org/thread/sprg0kq986pc2271dc3v2oxb1f9qx09j

2.2.8 jackson-annotations

基本信息

风险等级	安全

当前版本	2.12.6
所属语言	Java
发布厂商	com.fasterxml.jackson.core
名单类型	白名单
推荐版本	2.0.0-RC1
最新版本	2.17.1
是否开源	开源
下载源校验	成功
发布日期	2021-12-15
许可证	Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.9 httpmime

基本信息

风险等级	安全
当前版本	4.4.1
所属语言	Java
发布厂商	org.apache.httpcomponents
名单类型	白名单
推荐版本	4.0-alpha3
最新版本	4.5.14
是否开源	开源
下载源校验	成功
发布日期	2015-03-24
许可证	Apache-1.0,Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.10 jaxb-api

基本信息

风险等级	安全
当前版本	2.3.1
所属语言	Java
发布厂商	javax.xml.bind
名单类型	白名单
推荐版本	1.0

最新版本	2.3.1
是否开源	开源
下载源校验	成功
发布日期	2018-09-12
许可证	CDDL-1.1,GPL-2.0-with-classpath-exception
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.11 javax.activation-api

基本信息

风险等级	安全
当前版本	1.2.0
所属语言	Java
发布厂商	javax.activation
名单类型	白名单
推荐版本	1.2.0
最新版本	1.2.0
是否开源	开源
下载源校验	成功
发布日期	2017-09-07
许可证	CDDL-1.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.12 hamcrest-core

基本信息

风险等级	安全
当前版本	1.3
所属语言	Java
发布厂商	org.hamcrest
名单类型	白名单
推荐版本	1.1
最新版本	2.2
是否开源	开源
下载源校验	成功
发布日期	2012-07-10
许可证	BSD-3-Clause

引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.13 org.jacoco.agent

基本信息

风险等级	安全
当前版本	0.8.5
所属语言	Java
发布厂商	org.jacoco
名单类型	名单外
推荐版本	0.5.3.201107060350
最新版本	0.8.11
是否开源	开源
下载源校验	成功
发布日期	2019-10-12
许可证	Clips,EPL-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.14 jdom2

基本信息

风险等级	安全
当前版本	2.0.6.1
所属语言	Java
发布厂商	org.jdom
名单类型	白名单
推荐版本	2.0.6.1
最新版本	2.0.6.1
是否开源	开源
下载源校验	成功
发布日期	2021-12-07
许可证	TCL
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.15 ncoss-java-sdk

基本信息

风险等级	安全
当前版本	2.0.2-RELEASE
所属语言	Java
发布厂商	com.heredata.hos
名单类型	名单外
推荐版本	--
最新版本	--
是否开源	未知
下载源校验	成功
发布日期	
许可证	未声明
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.16 commons-logging

基本信息

风险等级	安全
当前版本	1.2
所属语言	Java
发布厂商	commons-logging
名单类型	白名单
推荐版本	1.0
最新版本	1.3.0
是否开源	开源
下载源校验	成功
发布日期	2014-07-06
许可证	Apache-1.0,Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.17 opentracing-api

基本信息

风险等级	安全

当前版本	0.33.0
所属语言	Java
发布厂商	io.opentracing
名单类型	白名单
推荐版本	0.2.0
最新版本	0.33.0
是否开源	开源
下载源校验	成功
发布日期	2019-05-06
许可证	Apache-1.0,Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.18 httpcore

基本信息

风险等级	安全
当前版本	4.4.1
所属语言	Java
发布厂商	org.apache.httpcomponents
名单类型	白名单
推荐版本	4.0-alpha3
最新版本	4.4.16
是否开源	开源
下载源校验	成功
发布日期	2015-03-15
许可证	Apache-1.0,Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.19 slf4j-api

基本信息

风险等级	安全
当前版本	1.7.30
所属语言	Java
发布厂商	org.slf4j
名单类型	白名单
推荐版本	1.1.0-beta0

最新版本	2.1.0-alpha1
是否开源	开源
下载源校验	成功
发布日期	2019-12-17
许可证	MIT
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.20 commons-collections4

基本信息

风险等级	安全
当前版本	4.1
所属语言	Java
发布厂商	org.apache.commons
名单类型	白名单
推荐版本	4.1
最新版本	4.5.0-M1
是否开源	开源
下载源校验	成功
发布日期	2015-11-26
许可证	Apache-1.0,Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.21 fastjson

基本信息

风险等级	安全
当前版本	1.2.83
所属语言	Java
发布厂商	com.alibaba
名单类型	白名单
推荐版本	2.0.0
最新版本	2.0.49
是否开源	开源
下载源校验	成功
发布日期	2022-05-23
许可证	Apache-2.0

引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.22 opentracing-noop

基本信息

风险等级	安全
当前版本	0.33.0
所属语言	Java
发布厂商	io.opentracing
名单类型	白名单
推荐版本	0.20.2
最新版本	0.33.0
是否开源	开源
下载源校验	成功
发布日期	2019-05-06
许可证	Apache-1.0,Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.23 opentracing-util

基本信息

风险等级	安全
当前版本	0.33.0
所属语言	Java
发布厂商	io.opentracing
名单类型	白名单
推荐版本	0.21.0
最新版本	0.33.0
是否开源	开源
下载源校验	成功
发布日期	2019-05-06
许可证	Apache-1.0,Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.24 slf4j-simple

基本信息

风险等级	安全
当前版本	1.7.30
所属语言	Java
发布厂商	org.slf4j
名单类型	名单外
推荐版本	1.0-beta7
最新版本	2.0.9
是否开源	开源
下载源校验	成功
发布日期	2019-12-17
许可证	MIT
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.25 jettison

基本信息

风险等级	安全
当前版本	1.5.4
所属语言	Java
发布厂商	org.codehaus.jettison
名单类型	白名单
推荐版本	1.5.4
最新版本	1.5.4
是否开源	开源
下载源校验	成功
发布日期	2023-03-14
许可证	Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.26 ini4j

基本信息

风险等级	安全

当前版本	0.5.4
所属语言	Java
发布厂商	org.ini4j
名单类型	白名单
推荐版本	0.3.1
最新版本	0.5.4
是否开源	开源
下载源校验	成功
发布日期	2015-02-17
许可证	Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.27 commons-codec

基本信息

风险等级	安全
当前版本	1.9
所属语言	Java
发布厂商	commons-codec
名单类型	白名单
推荐版本	1.3
最新版本	1.17.0
是否开源	开源
下载源校验	成功
发布日期	2013-12-21
许可证	Apache-1.0,Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.28 jackson-core

基本信息

风险等级	安全
当前版本	2.12.6
所属语言	Java
发布厂商	com.fasterxml.jackson.core
名单类型	名单外
推荐版本	2.0.0-RC1

最新版本	2.17.1
是否开源	开源
下载源校验	成功
发布日期	2021-12-15
许可证	Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.29 jackson-mapper-asl

基本信息

风险等级	安全
当前版本	0.9.6
所属语言	Java
发布厂商	org.codehaus.jackson
名单类型	名单外
推荐版本	0.9.6
最新版本	1.9.13
是否开源	开源
下载源校验	成功
发布日期	2009-01-15
许可证	Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.30 junit

基本信息

风险等级	安全
当前版本	4.13.2
所属语言	Java
发布厂商	junit
名单类型	白名单
推荐版本	4.0
最新版本	4.13.2
是否开源	开源
下载源校验	成功
发布日期	2021-02-14
许可证	Clips,EPL-1.0

引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.31 jackson-core-asl

基本信息

风险等级	安全
当前版本	1.9.13
所属语言	Java
发布厂商	org.codehaus.jackson
名单类型	白名单
推荐版本	0.9.6
最新版本	1.9.13
是否开源	开源
下载源校验	成功
发布日期	2013-07-15
许可证	Apache-2.0
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

2.2.32 lombok

基本信息

风险等级	安全
当前版本	1.18.12
所属语言	Java
发布厂商	org.projectlombok
名单类型	白名单
推荐版本	0.9.3
最新版本	1.18.30
是否开源	开源
下载源校验	成功
发布日期	2020-02-07
许可证	MIT
引入方式	
漏洞分布	超危 0、高危 0、中危 0、低危 0

引入来源

漏洞列表（0）

3 漏洞

3.1 漏洞风险列表

表 3-1 漏洞风险列表

漏洞名称	CVE 编号	风险等级	漏洞类型
Spring Framework 代码注入漏洞	CVE-2022-22965	超危	代码注入
CVE-2023-2976	CVE-2023-2976	高危	CWE-552
gson 代码问题漏洞	CVE-2022-25647	高危	代码问题
FasterXML jackson-databind 缓冲区错误漏洞	CVE-2020-36518	高危	缓冲区错误
CVE-2022-42004	CVE-2022-42004	高危	CWE-502
CVE-2022-42003	CVE-2022-42003	高危	CWE-502
CVE-2023-33202	CVE-2023-33202	中危	CWE-400
Vmware Spring Framework 安全特征问题漏洞	CVE-2022-22968	中危	安全特征问题
CVE-2023-33201	CVE-2023-33201	中危	CWE-295
Apache POI 代码问题漏洞	CVE-2019-12415	中危	代码问题
Spring Framework 输入验证错误漏洞	CVE-2022-22971	中危	输入验证错误
Apache POI 资源管理错误漏洞	CVE-2022-26336	中危	资源管理错误
CVE-2023-20863	CVE-2023-20863	中危	CWE-917
CVE-2023-20861	CVE-2023-20861	中危	NVD-CWE-noinfo
Spring Framework 输入验证错误漏洞	CVE-2022-22970	中危	输入验证错误
Google Guava 代码问题漏洞	CVE-2018-10237	中危	代码问题
Apache HttpClient 安全漏洞	CVE-2020-13956	中危	其他
Google Guava 访问控制错误漏洞	CVE-2020-8908	低危	访问控制错误

4 许可证

4.1 许可证列表

表 4-1 许可证风险列表

许可证	风险等级	类型	OSI	FSF	SPDX	影响组件数
EPL-1.0	中风险	弱著佐权型	是	是	是	1
CDDL-1.1	中风险	弱著佐权型	否	否	是	1
CDDL-1.0	中风险	弱著佐权型	是	是	是	1
EPL-2.0	中风险	弱著佐权型	是	是	是	1
MIT	低风险	宽松型	是	是	是	3
TCL	低风险	宽松型	否	否	是	1
Apache-1.0	低风险	宽松型	否	是	是	9
Apache-2.0	低风险	宽松型	是	是	是	21

BSD-3-Clause	低风险	宽松型	是	是	是	1
未声明	未知				是	2
GPL-2.0-with-classpath-exception	未知		否	否	是	1
Clips	未知		否	否	是	2

4.2 兼容性分析

5 风险评分

1.指标名称：使用黑名单组件数量		指标类型：加减分	
指标口径： 得分方法：线性递减法			
风险评估对象	**风险数值**	**最终得分**	**结果**
CMStore	15	不扣分	无

2.指标名称：安全漏洞数量（等级）		指标类型：管理 KPI	
指标口径：风险等级 得分方法：等级法+线性法 满分：60 超危风险数值小于等于：100 得最高分：20 分 风险数值大于：120 得最低分：10 分 高危风险数值小于等于：85 得最高分：10 分 风险数值大于：100 得最低分：5 分 中危风险数值小于等于：75 得最高分：20 分 风险数值大于：85 得最低分：10 分 低危风险数值小于等于：65 得最高分：10 分 风险数值大于：70 得最低分：5 分			
风险评估对象	**风险数值**	**最终得分**	**结果**
CMStore	超危：1 高危：5 中危：11 低危：1	60.0	无

3.指标名称：许可证评分（等级）	指标类型：管理 KPI

指标口径：风险等级 得分方法：等级法+线性法 满分：20 高风险风险数值小于等于：100 得最高分：10 分 风险数值大于：120 得最低分：5 分 中风险风险数值小于等于：150 得最高分：5 分 风险数值大于：200 得最低分：3 分 低风险风险数值小于等于：75 得最高分：5 分 风险数值大于：85 得最低分：3 分
指标口径：使用场景 得分方法：等级法+线性法 满分：10 涉及场景数大于等于：5 得最高分：10 分 涉及场景数小于：2 得最低分：5 分
指标口径：传染性 得分方法：等级法+线性法 满分：10 无传染时 得最高分：10 分 强传染时 得最低分：5 分

风险评估对象	风险数值	最终得分	结果
CMStore	风险等级： 高风险：0 中风险：4 低风险：5 使用场景： 可使用场景数：0 传染性：无传染	35.0	无