



墨菲安全

MURPHYSEC

以开发者为核心

行业领先的软件供应链安全平台

# 软件安全检测报告&SBOM导出

2024.01

# 关于墨菲安全



**懂企业** 超十年甲方应用安全建设经验，核心团队来自百度、华为、平安、招行、贝壳；

**产品技术领先** 顶级的漏洞研究及应用安全实践经验，创始人曾在乌云主导国内首款检测SaaS产品TangScan；

**和客户一起成长** 软件及应用安全重运营，墨菲安全理念是伴随客户安全业务一起成长，持续迭代创新；

## 核心团队



### 创始人&CEO 章华鹏

前百度安全架构师，乌云产品合伙人  
top10白帽子，首款SaaS产品tangscan  
独立发现国内外企业数百个严重漏洞



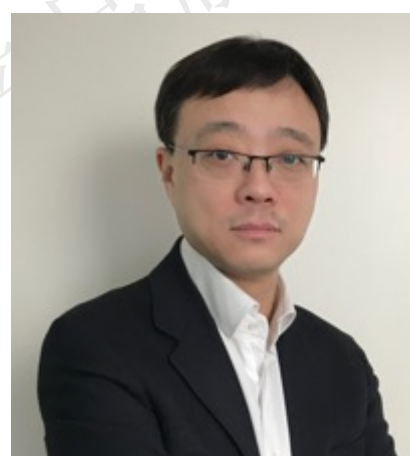
### 联创&实验室负责人 欧阳强斌

前百度、贝壳资深安全工程师  
曾负责百度蓝军攻防团队  
贝壳基础安全团队负责人



### 联创&工程负责人 宇佰超

前华为、贝壳工程技术专家  
曾负责华为多款安全产品的研发及架构设计，贝壳零信任架构负责人



### 合伙人&COO 周欣

前梆梆安全COO，负责营销工作  
在安全市场营销及销售方面超过二十年的丰富经验，专业的客户服务能力



### 联创&方案负责人 崔泷跃

前平安、招行及百度资深安全工程师  
超过十年的开发安全、DevSecOps及SDL方面的落地经验



### 联创&产品负责人 车志远

前百度、贝壳资深安全工程师  
曾负责单一企业超过50万用户的企业级安全产品的设计及落地



# 部分典型客户案例



## 互联网



## 金融业



## 运营商



## 能源及制造



## 监管合作





# 全球首个软件供应链安全技术社区 实力验证



500+ 顶级开源项目通过OSCS社区一键修复安全漏洞

<p>theonedev/onedev ☆ 9897 ▼ 667 OSCS白帽子为项目修复了 5 个安全风险 平均处理时长 0.1 h</p>	<p>apache/thrift ☆ 9409 ▼ 3880 OSCS白帽子为项目修复了 2 个安全风险 平均处理时长 42 h</p>	<p>ssssssss-team/spider-flow ☆ 7352 ▼ 1390 OSCS白帽子为项目修复了 24 个安全风险 平均处理时长 0.8 h</p>
<p>wildfirechat/im-server ☆ 6861 ▼ 1607 OSCS白帽子为项目修复了 1 个安全风险 平均处理时长 1.2 h</p>	<p>codingapi/tx-icn ☆ 4173 ▼ 1465 OSCS白帽子为项目修复了 12 个安全风险 平均处理时长 14.2 h</p>	<p>apache/hudi ☆ 3614 ▼ 1665 OSCS白帽子为项目修复了 1 个安全风险 平均处理时长 53.8 h</p>

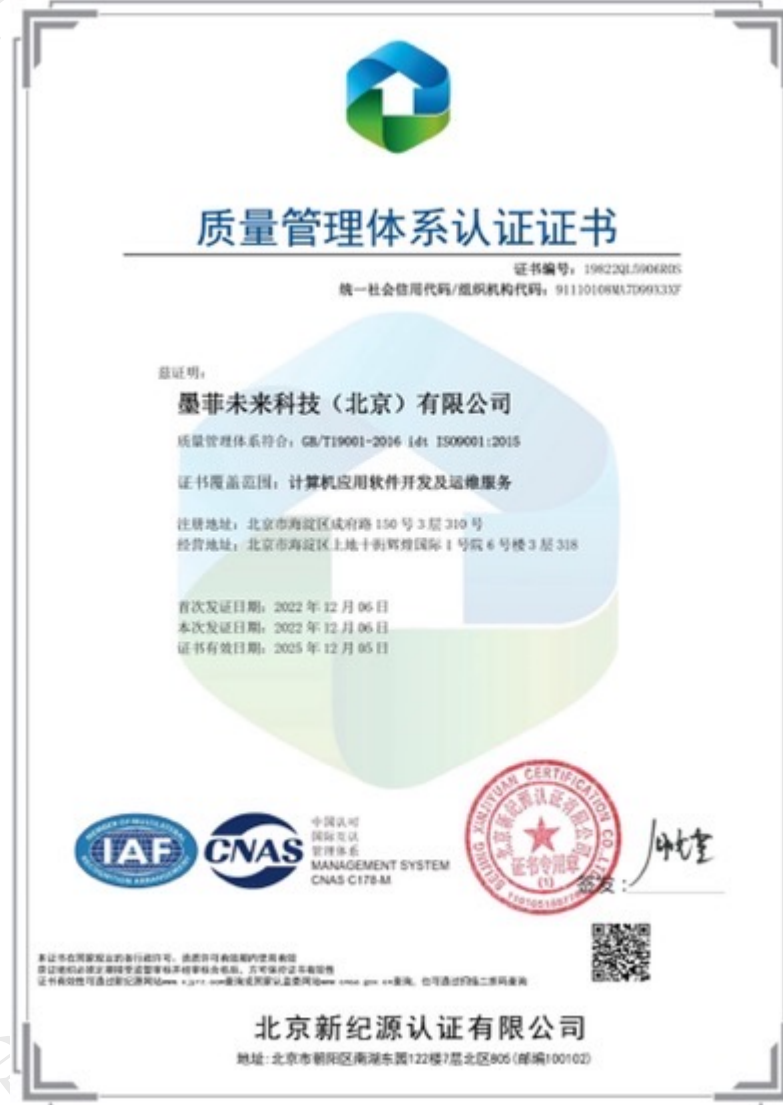
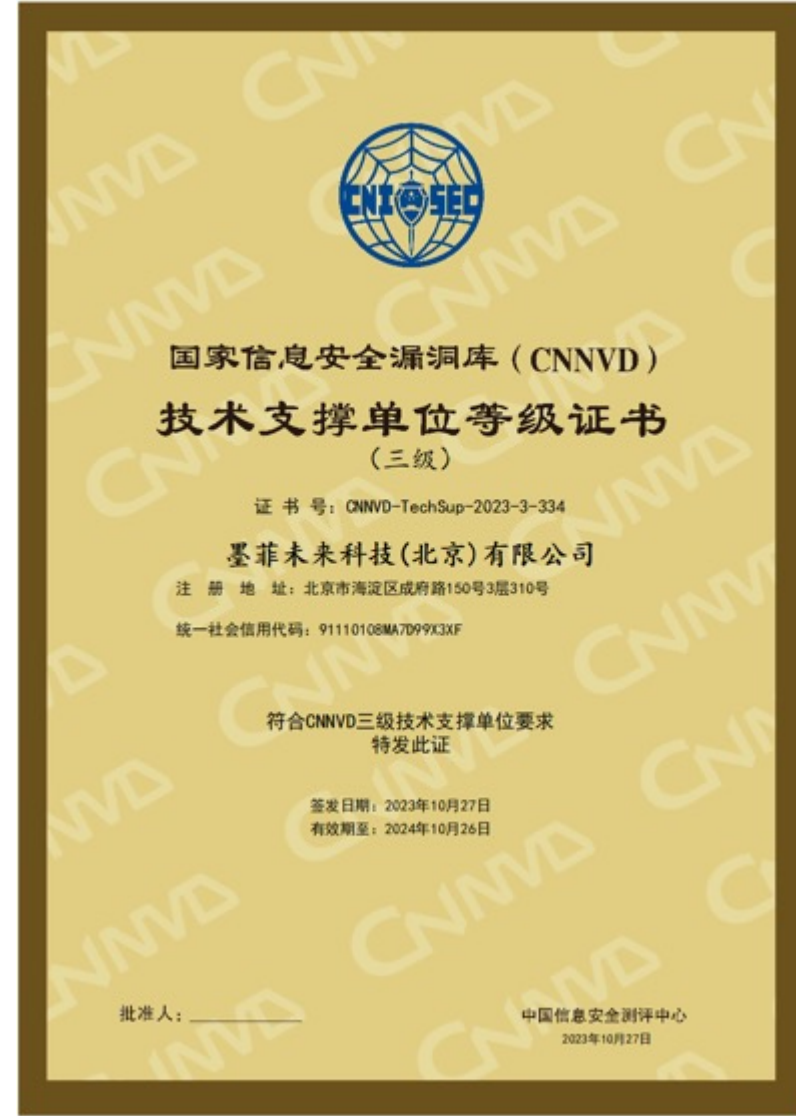
**36万** 累计检测项目数  
**750万** 累计发现漏洞数  
**41万** 知识库覆盖漏洞数  
**8000万** 知识库覆盖组件数

超过20000个开发者正在使用墨菲安全SaaS产品

<p>Zhfuln 2022-10-13</p>	<p>liuxuxiang 2022-10-21</p>	<p>eurrio 2022-10-13</p>	<p>s024wh 2022-10-25</p>	<p>Master_Sky 2022-10-25</p>
<p>Kunni 2022-10-14</p>	<p>denglunfuren 2022-10-21</p>	<p>徐晓伟 2022-10-13</p>	<p>猪娃娃 2022-10-13</p>	<p>TopScrew 2022-10-13</p>



# 资质及荣誉





# 墨菲安全 八大场景解决方案



## 开源组件安全风险治理

适用场景：因监管及安全事件，需开展开源安全/合规治理  
相关监管：银保监、公安部、工信部、证监会等  
产品特性：漏洞可达性分析、修复兼容性评估、网关准入准出  
适用行业：金融/运营商/互联网/能源/关基/制造 等  
典型客户：快手、中国移动、中国银行、中国电信、兴业证券、小红书

## 资产及漏洞投毒应急响应

适用场景：突发0day及投毒事件应急响应，避免勒索及数据泄露  
相关监管：公安部、网信办、银保监等  
产品特性：0day首发预警、投毒情报、25+独家漏洞分析字段  
适用行业：互联网/金融/运营商/能源/关基 等  
典型客户：蚂蚁、美团、阿里、腾讯、国家电网、理想汽车、微众银行

## 开源组件许可证风险治理

适用场景：企业产品出海/交付甲方/对外开源担心出现许可证合规风险  
相关监管：知识产权保护法、甲方安全要求、开源社区准则  
产品特性：代码片段级溯源、二进制及固件成分分析  
适用行业：车企/IoT厂商/软硬件出海企业/先进制造 等  
典型客户：理想、高德、小米、美团、道通科技

## 车企/智能制造安全及合规

适用场景：面临国内外严格的标准要求，对许可证及漏洞风险管理严格  
相关监管：欧盟R155、国内车企强标、国内外知识产权保护法  
产品特性：全球领先漏洞知识库、代码片段级溯源、二进制及固件分析  
适用行业：智能网联车/先进制造 等  
典型客户：理想、小米、道通科技

# 墨菲安全 八大场景解决方案



## 商业软件供应链安全治理

适用场景：企业大量外采软件供应商漏洞及数据泄露导致企业受影响  
相关监管：银保监、公安部、工信部、证监会等  
产品特性：网关准入准出、商业软件二进制安全检测、软件供应商情报  
适用行业：金融/运营商/能源/关基/互联网 等  
典型客户：中国移动、中国银行、中国电信、兴业证券、广发银行

## 护网资产及风险排查

适用场景：护网前对存在安全漏洞及隐患的供应链资产排查整改  
相关监管：公安部、通管局  
产品特性：资产识别、0day知识库、POC、快速修复  
适用行业：金融/运营商/能源/关基 等  
典型客户：中国移动、天翼云、中国银行等

## 软件安全检测报告及SBOM输出

适用场景：软件厂商在投标及交付产品时需带安全检测报告及SBOM  
相关监管：甲方企业安全要求  
产品特性：行业认可的检测报告、SBOM导出、报告导出  
适用行业：软件厂商 等  
典型客户：道通科技、广州嘉为、沃丰科技

## 监管软件安全产品检测及认证

适用场景：作为监管及认证单位，需要自动化对产品进行检测认证  
相关监管：各类国标  
产品特性：简单易用、结果准确、覆盖率高、可解释性强  
适用行业：监管、检测认证机构 等  
典型客户：信通院、公安部、金融认证中心 等



# 目录



专业、专注、可靠

01

背景情况

02

解决方案

03

产品介绍

04

客户案例



# 背景介绍

为明确软件供应链安全责任，企业采购部门要求供应商提供SBOM及安全检测报告，并在准入环节进行安全审查



银行



证券



保险



运营商



能源及制造



车企

甲方  
开源  
审查  
流程



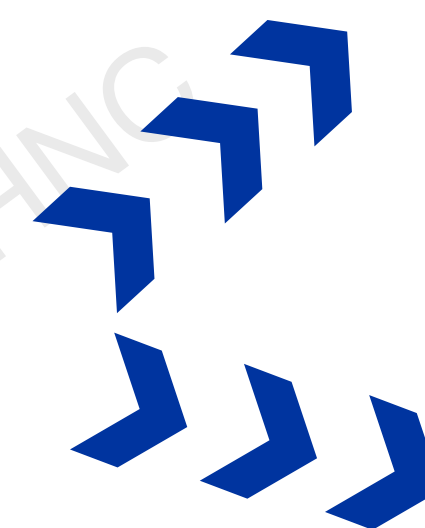
待采购  
商业软件



上传扫描  
二进制安装包



漏洞检测报告  
SBOM清单



反馈采购评分  
厂商整改



记录进  
资产台账



# 供应商安全报告痛点



1

## 检测报告客户认可度差

- 报告中组件资产不全
- 组件资产引入信息不准
- 客户自查发现的风险未提前发现

2

## 检出风险处置成本高

- 检测出大量安全问题，影响不明确
- 漏洞修复方案不明确
- 漏洞修复兼容性难评估



# 目录



专业、专注、可靠

01

背景情况

02

解决方案

03

产品介绍

04

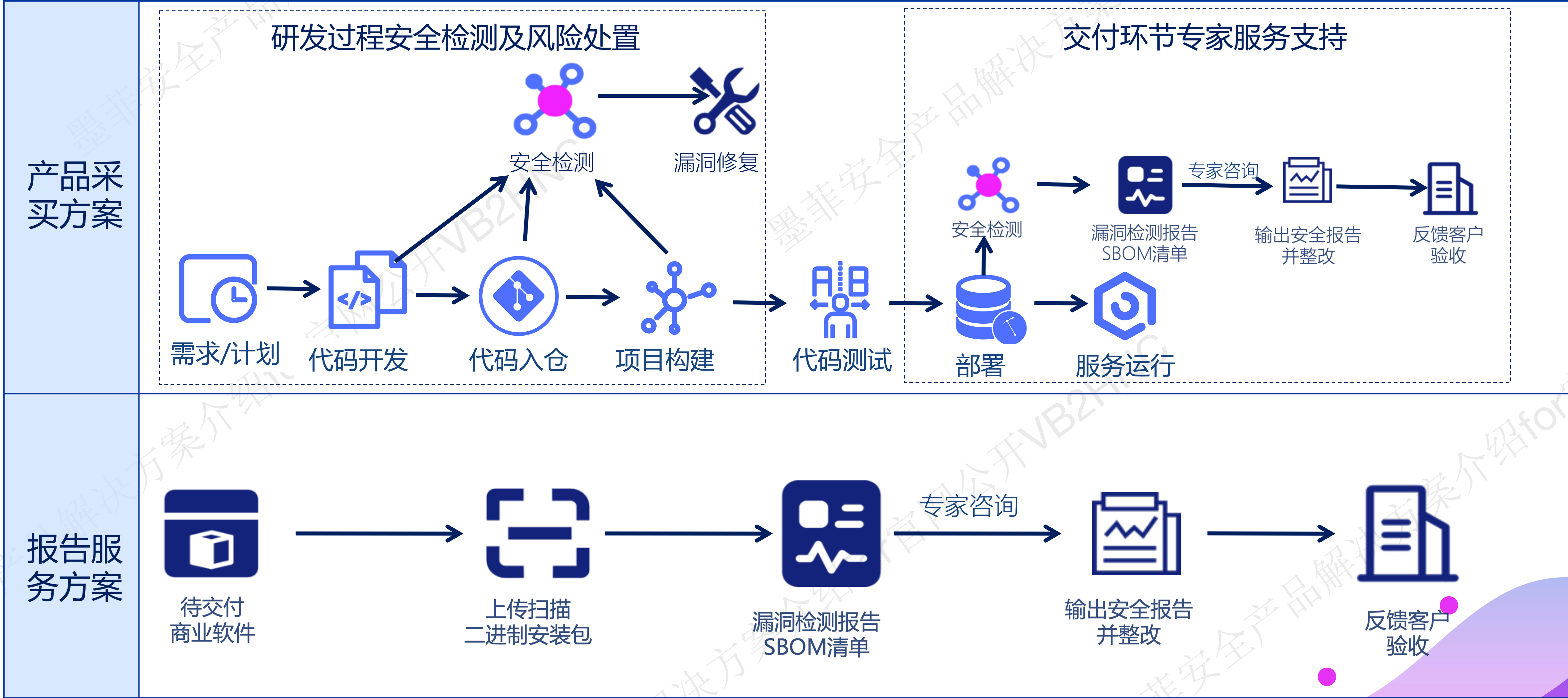
客户案例



# 墨菲安全检测报告及SBOM输出方案

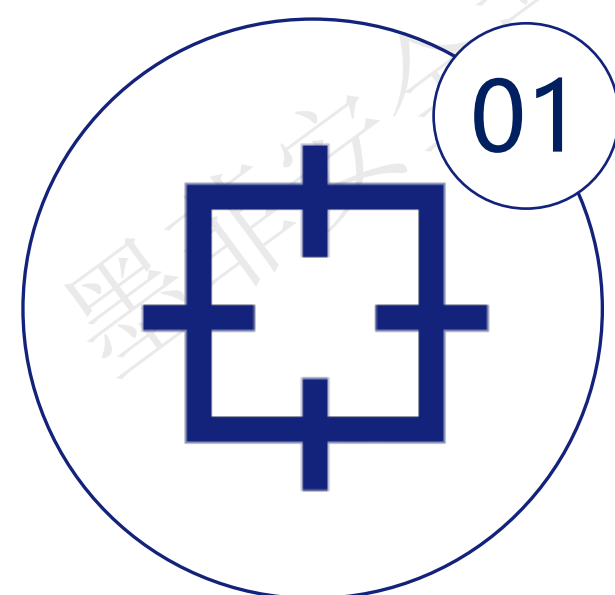


专业检测工具结合资深安全专家审核输出甲方认可的安全检测报告





# 三大特性 解决安全报告核心痛点



01

## 高准SBOM识别

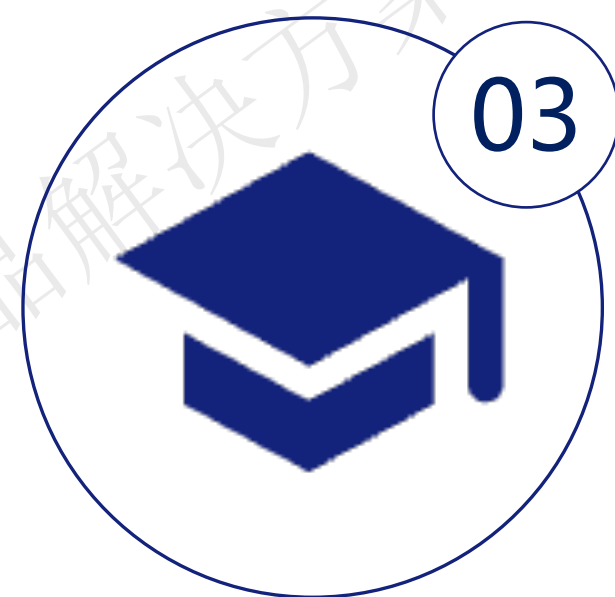
- 源代码SBOM识别
- 二进制SBOM识别
- 容器镜像SBOM识别



02

## 漏洞快速修复

- 漏洞真实影响分析
- 漏洞升级兼容性评估
- IDE插件一键修复
- 修复效率提升20倍



03

## 专家服务支持

- 专家提供专业整改方案
- 专家复核报告，保证通过



# 目录



专业、专注、可靠

01

背景情况

02

解决方案

03

产品介绍

04

客户案例



# 供应链安全检测及SBOM导出





# 专业检测报告，多行业客户认可





金融证券



中国银行  
BANK OF CHINA



兴业证券  
INDUSTRIAL SECURITIES



中国平安  
PING AN  
保险·银行·投资



大家保险



能源及制造



国家电网  
STATE GRID



理想



中国建筑  
CHINA STATE CONSTRUCTION



中国移动  
China Mobile



中国电信  
CHINA TELECOM  
世界触手可及



天翼云

软件成分分析报告

**基本信息**

检测编号	1730012772121219074
项目名称	RuoYi-4.6.1.rar
项目地址	-
检测分支	-
检测方式	标准扫描
主体语言	Java
项目负责人	sunhui
检测人员	sunhui
所属团队	sunhui的团队
团队负责人	sunhui
检测时间	2023-12-08 06:36:57
检测耗时	150.63s

**组件概览**

组件数量	强烈建议修复	建议修复	可选修复	无风险
208	3	32	17	156

**漏洞概览**


漏洞数量	严重	高危	中危	低危	可POC	CVE收录
103	15	34	46	8	38	6

**许可证概览**

许可证数量	许可证类型	高风险
8	8	0

**组件相关统计图表**

组件风险等级统计:



208个

可触发漏洞组件:

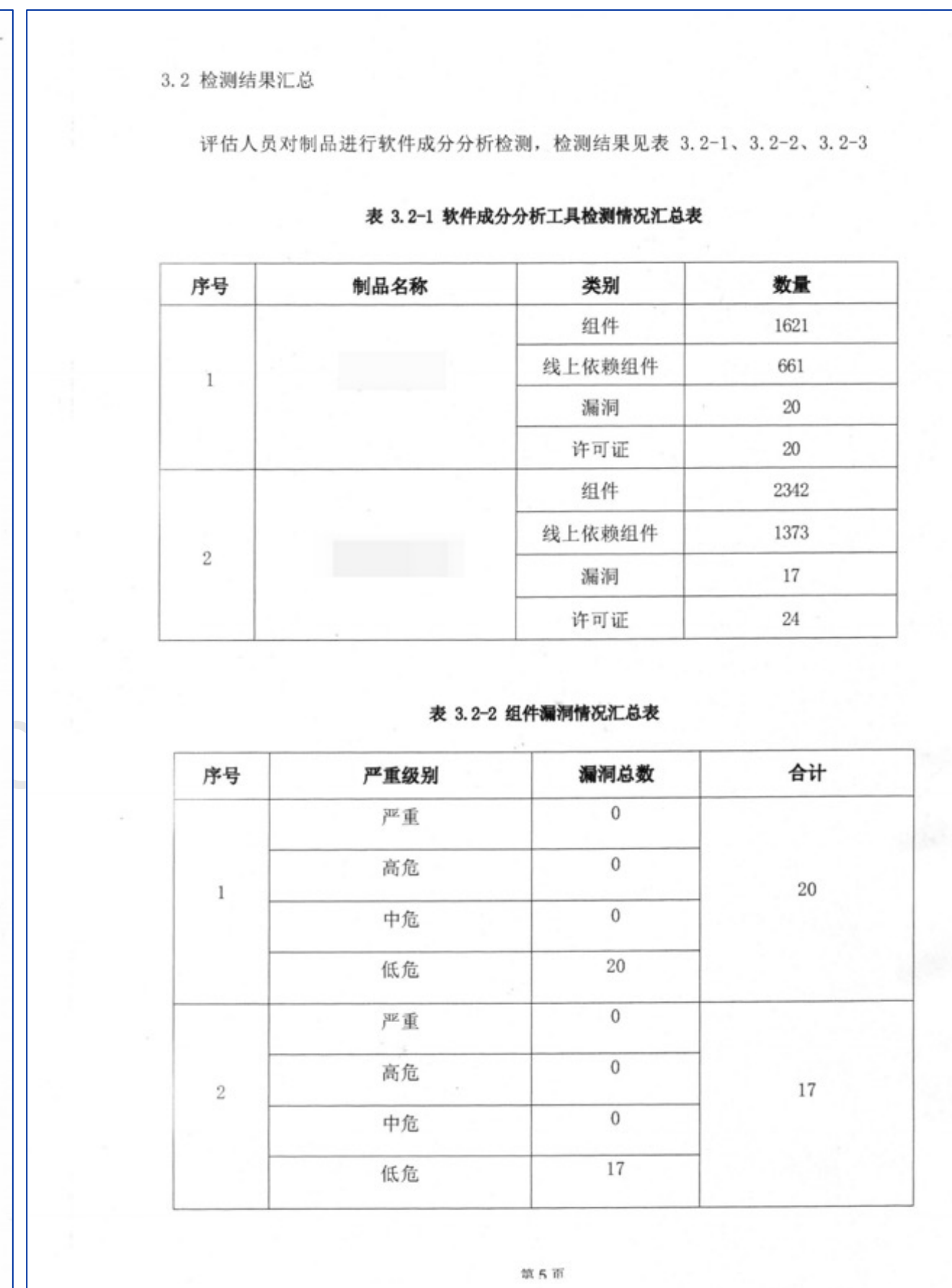
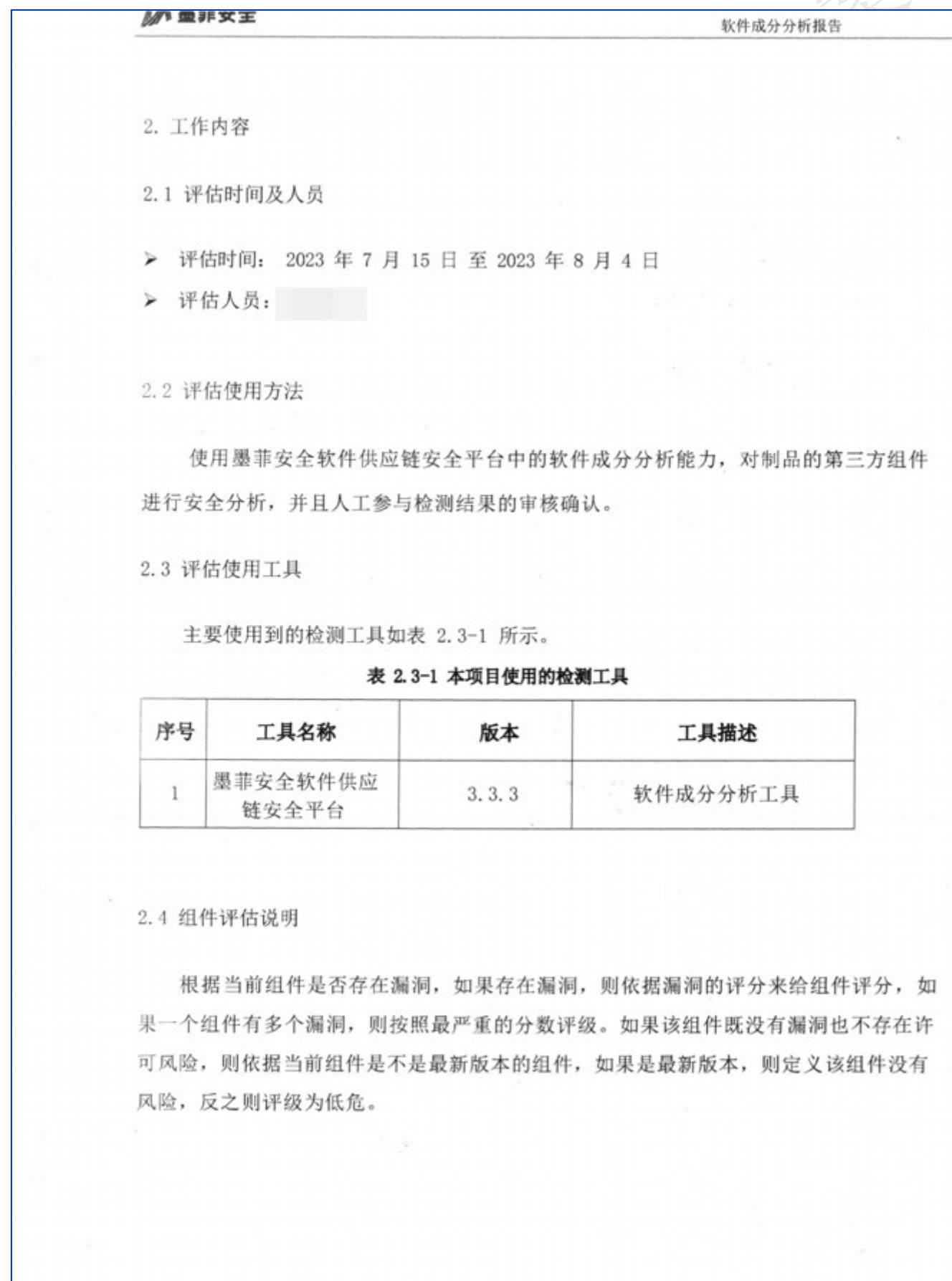
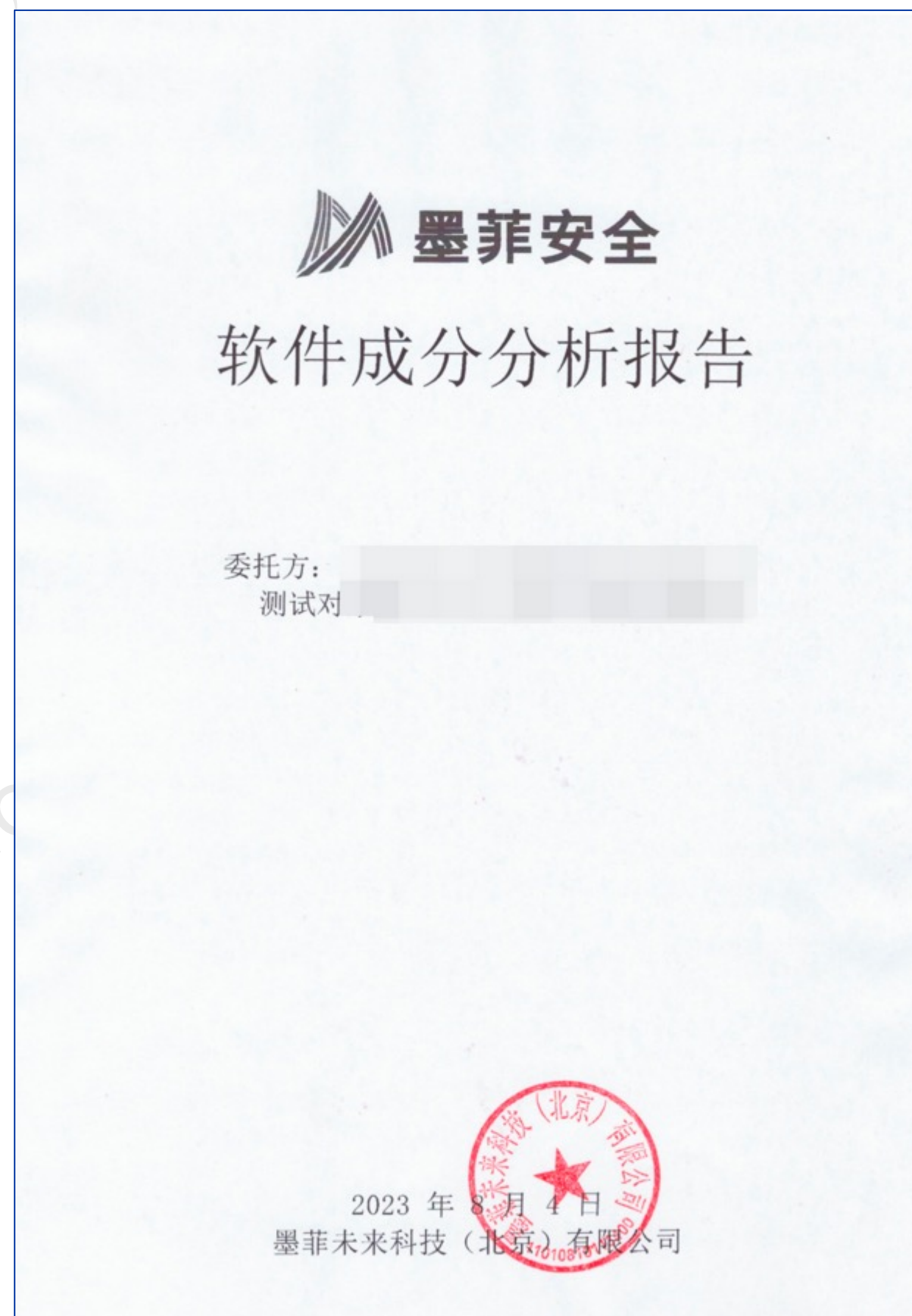
- 强烈建议修复: 1.44%
- 建议修复: 15.38%
- 可选修复: 8.17%
- 安全: 75.00%

编号	漏洞标题	漏洞编号	等级	漏洞类型	攻击成本/范围	是否可触发	漏洞标签	影响组件	漏洞链接
3/2	RuoYi 安全漏洞	CVE-2023-27025	高危	下载代码缺少完整性检查	远程	/		该项目中受影响的组件: com.ruoyi.ruoyi-quartz@4.6.1	https://www.oscs1024.com/hd/MPS-2023-6193
3/3	Apache Tomcat 输入验证错误漏洞	CVE-2023-46589	高危	HTTP请求走私	远程	/		该项目中受影响的组件: org.apache.tomcat.embed:tomcat-embed-core@9.0.41 方案1; 将组件升级为9.0.83版本 方案2; 将组件升级为9.0.89版本	https://www.oscs1024.com/hd/MPS-67md-8wr2
3/4	commons-fileupload/commons-fileupload 存在信息暴露漏洞	MPS-2022-16625	中危	未授权敏感信息披露	远程	小	CVE未收录漏洞	该项目中受影响的组件: commons-fileupload:commons-fileupload@1.2.1 方案1; 将组件升级为1.5版本 方案2; 将组件升级为1.5版本 方案3; 将组件升级为1.3.1-jenkins-1版本	https://www.oscs1024.com/hd/MPS-2022-16625
3/5	snakeYAML <2.0 存在反序列化漏洞	CVE-2022-1471	高危	反序列化	远程	小	可触发漏洞	该项目中受影响的组件: org.yaml:snakeyaml@1.25 方案1; 将组件升级为2.0版本 方案2; 将组件升级为2.0版本	https://www.oscs1024.com/hd/MPS-2022-9425
3/6	MyBatis <3.5.6 存在反序列化漏洞	CVE-2020-28945	高危	反序列化	远程	小	/	该项目中受影响的组件: org.mybatis:mybatis@3.5.5 方案1; 将组件升级为3.5.12版本 方案2; 将组件升级为3.5.6版本	https://www.oscs1024.com/hd/MPS-2020-14133
3/7	【存在争议】FasterXML jackson-databind 代码问题漏洞	CVE-2023-35116	中危	不加载或调节的资源分配	本地	可触发漏洞	可POC, 线上依赖	该项目中受影响的组件: com.fasterxml.jackson.core:jackson-databind@2.10.5.1 方案1; 将组件升级为2.13.5版本	https://www.oscs1024.com/hd/MPS-21bp-p8y2
3/8	Pivotal Spring Framework 安全限制绕过漏洞	CVE-2022-22968	中危	大小写敏感处理不当	远程	小	/	该项目中受影响的组件: org.springframework:spring-context@5.2.12 RELEASE 方案1; 将组件升级为5.2.23 RELEASE版本 方案2; 将组件升级为5.2.23 RELEASE版本	https://www.oscs1024.com/hd/MPS-2022-1098
3/9	bootstrap-table XSS	MPS-2022-54370	中危	XSS	远程	/	CVE未收录漏洞	该项目中受影响的组件: bootstrap-table@1.18.2	https://www.oscs1024.com/hd/MPS-2022-54370
4/0	Spring Framework <6.0.0 远程代码执行漏洞	CVE-2016-100027	严重	反序列化	远程	一般	/	该项目中受影响的组件: org.springframework:spring-web@5.2.12 RELEASE 方案1; 将组件升级为6.0.14版本 方案2; 将组件升级为5.2.23 RELEASE版本	https://www.oscs1024.com/hd/MPS-2020-0057
4/1	Apache Log4j SmtppAppender证书验证不当漏洞	CVE-2020-9488	低危	证书验证不当	远程	一般	/	该项目中受影响的组件: log4j:log4j@1.2.1.2 方案1; 将组件升级为1.2.13版本	https://www.oscs1024.com/hd/MPS-2020-6684
4/2	Apache Tomcat 远程代码执行漏洞	CVE-2021-25329	高危	代码注入	本地	一般	/	该项目中受影响的组件: org.apache.tomcat.embed:tomcat-embed-core@9.0.41 方案1; 将组件升级为9.0.83版本 方案2; 将组件升级为9.0.89版本	https://www.oscs1024.com/hd/MPS-2021-2466
4/3	FasterXML jackson-databind <2.1.4.0-rc1 拒绝服务漏洞	CVE-2022-42003	中危	拒绝服务	小	可触发漏洞	可POC, 线上依赖	该项目中受影响的组件: com.fasterxml.jackson.core:jackson-databind@2.10.5.1 方案1; 将组件升级为2.13.5版本	https://www.oscs1024.com/hd/MPS-2022-58653
4/4	RuoYi SQL注入漏洞	CVE-2022-48114	严重	SQL注入	远程	/		该项目中受影响的组件: com.ruoyi.ruoyi-common@4.6.1	https://www.oscs1024.com/hd/MPS-2022-69927
4/5	Apache Commons FileUpload DiskFileItem 任意文件写入漏洞	CVE-2013-2186	高危	输入验证不当	远程	小	/	该项目中受影响的组件: commons-fileupload:commons-fileupload@1.2.1 方案1; 将组件升级为1.5版本 方案2; 将组件升级为1.5版本 方案3; 将组件升级为1.3.1-jenkins-1版本	https://www.oscs1024.com/hd/MPS-2013-4267
4/6	SnakeYAML <1.26 存在 Billion laughs 漏洞	CVE-2017-18640	高危	拒绝服务	远程	小	可触发漏洞	该项目中受影响的组件: org.yaml:snakeyaml@1.25 方案1; 将组件升级为2.0版本 方案2; 将组件升级为2.0版本	https://www.oscs1024.com/hd/MPS-2019-16129
4/7	Apache Tomcat 条件竞争漏洞	CVE-2021-43980	低危	竞争条件	远程	一般	/	该项目中受影响的组件: org.apache.tomcat.embed:tomcat-embed-core@9.0.41 方案1; 将组件升级为9.0.83版本 方案2; 将组件升级为9.0.89版本	https://www.oscs1024.com/hd/MPS-2021-37218
4/8	snakeYAML <1.31 存在基于堆栈的缓冲区溢出漏洞	CVE-2022-38749	中危	拒绝服务	远程	小	可触发漏洞	该项目中受影响的组件: org.yaml:snakeyaml@1.25 方案1; 将组件升级为2.0版本 方案2; 将组件升级为2.0版本	https://www.oscs1024.com/hd/MPS-2022-56881
4/9	VMware Spring Boot 安全漏洞	CVE-2023-34055	中危		远程	/		该项目中受影响的组件: org.springframework:spring-boot@2.2.13 RELEASE 方案1; 将组件升级为2.7.18版本	https://www.oscs1024.com/hd/MPS-0q4t-ivum



# 资深专家支持，保证通过甲方审查

- ✓ 上百家客户过审经验
- ✓ 超十年甲方安全建设经验
- ✓ 信息安全执业资质





# 目录



专业、专注、可靠

01

背景情况

02

解决方案

03

产品介绍

04

客户案例



# 某头部软件厂商W案例

## 客户痛点

- ① 甲方要求客户投标时出示软件安全检测报告及SBOM
- ② 之前找其他厂商做的安全报告客户不认可
- ③ 出示安全报告时发现大量安全问题，无法及时修复

## 挑战

- ① 时间紧，任务重，需要检测的代码规模庞大，客户要求高
- ② 检测出来的大量安全问题不知如何修复

## 解决方案

- ① 基于墨菲安全的软件检测平台输出安全检测报告
- ② 由墨菲安全的技术专家指导修复安全问题并确认报告有效性



## 收益

- ① 检测发现的严重及高危问题及时得到修复
- ② 顺利通过客户的验收，客户表示十分满意



# 公司发展历程



来自百度、华为为主的核心团队组建，启动墨菲安全漏洞知识库建设



完成顶级投资机构红杉资本数千万天使轮融资



墨菲安全签约十数家互联网、金融、运营商客户



墨菲安全入选国家高新技术企业，签约数十家互联网、金融、运营商客户

2020.05

2021.09

2021.11

2022.03

2022.12

2023.05

2023.12

产品v1.0正式发布，适配主流DevOps流程及工具

产品2.0发布，接入平安、快手等第一批头部客户

墨菲安全软件供应链安全v3版本发布，全球首发可达性风险及兼容性评估技术





# 联系我们



公司地址:

北京市海淀区百旺弘祥(弘祥1989)文创园

联系人:

杨女士

联系电话:

400 180 9568

官网:

<https://www.murphysec.com/>

