|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | |  |
|  | | |
|  | | |
| 方圆ok1 | | | |
|  | **重庆超体科技有限公司**  **智慧关务**  鲲鹏认证安全合规测试报告 | |  |
|  | |
| **文档版本** | **01** |
| **发布日期** | **2020-07-07** |
|  | |
| 华为技术有限公司 | |
|  | | |

|  |
| --- |
| 版权所有 © 华为技术有限公司 2019。 保留一切权利。  非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。  商标声明  和其他华为商标均为华为技术有限公司的商标。  本文档提及的其他所有商标或注册商标，由各自的所有人拥有。  注意  您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。  由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。 |

|  |  |
| --- | --- |
| 华为技术有限公司 | |
| 地址： | 深圳市龙岗区坂田华为总部办公楼 邮编：518129 |
| 网址： | https://www.huaweicloud.com/ |

1. 前 言

修改记录

| 文档版本 | 修改说明 | 发布日期 | 作者 | 签发 |
| --- | --- | --- | --- | --- |
| V1.0 | 第一次发布 | 2020-07-07 | XXX | XXX |

目录

[1 前 言 2](#_Toc9043)

[1 安全测试概述 4](#_Toc23328)

[1.1 安全测试范围与指导 4](#_Toc11696)

[1.2 安全测试策略 4](#_Toc13579)

[2 安全测试环境信息 5](#_Toc6916)

[2.1测试环境清单 5](#_Toc18796)

[2.2被测软件版本信息 5](#_Toc24560)

[3 安全测试工具描述 6](#_Toc12061)

[3.1 安全测试工具 6](#_Toc24989)

[3.2安全测试时间和测试人员 6](#_Toc8566)

[4测试执行 7](#_Toc30093)

[4.1安全测试结果综述及关键风险 7](#_Toc12630)

[4.1.1 产品安全红线总体达成目标 7](#_Toc15612)

[4.1.2 产品web、主机扫描中高风险汇总和跟踪 7](#_Toc26491)

[4.1.3 安全测试用例执行结果统计表 7](#_Toc8285)

[4.1.4防暴力破解机制检测 8](#_Toc10889)

[5安全测试记录 9](#_Toc5050)

[5.1安全测试日志 9](#_Toc3705)

[6安全测试总结 10](#_Toc21239)

[6.1测试总结 10](#_Toc8257)

[6.2结果确认 10](#_Toc32072)

# 1 安全测试概述

## 1.1 安全测试范围与指导

华为云市场安全合规要求以及测试指导。



## 安全测试策略

1. 安全测试以《华为云市场安全合规要求(试行版)》的要求为测试基准，对系统组件安全、第三方组件安全、系统安全配置及Web容器进行安全测试。
2. SaaS现网商用环境安全扫描安全测试策略，避免影响现网商用环境，只做Web安全扫描，不做主机安全扫描。
3. 镜像类产品需对主机和应用同时做安全扫
4. 数据库类产品需针对主机做安全扫描
5. 软件下载类产品安全测试策略，需做通用web扫描及主机安全扫描

注：根据产品特性选择相应的测试策略

# 2 安全测试环境信息

## 2.1测试环境清单

本次测试环境资源清单如下表所示

表格 2‑1安全测试环境清单

|  | 相关说明 | 数量 | 配置参数 | 备注 |
| --- | --- | --- | --- | --- |
| XXX（产品名称） | ECS弹性云服务器 | 1 | 系统版本：openEuler 20.03 64bit with ARM  处理器 kc1.4xlarge.2 | 16vCPUs | 32GB  硬盘：100G  共享带宽：20M | 华为云提供 |
| 数据库服务器 | 1 | 数据库版本：MySQL5.7.27-aarch64  处理器： kc1.2xlarge.4 | 8vCPUs | 32GB  共享带宽：20M  磁盘：40 GB | 华为云提供 |
| Redis数据缓存服务 | 1 | 系统版本：Redis 5.0 for Arm|DRAM  处理器：kc1.4xlarge.2 | 16vCPUs | 32GB  规格：0.125G  共享带宽：20M | 华为云提供 |

## 2.2被测软件版本信息

本次测试被测软件版本信息如下表

表格 2‑2被测软件版本信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **使用组件** | **版本号** | **OS版本** | **备注** |
| 1 | 智慧关务 | V1.0 | openEuler 20.03 64bit with ARM |  |

# 3 安全测试工具描述

## 3.1 安全测试工具

描述本次测试使用了哪些测试工具。

表格 2‑1安全测试工具

|  |  |  |  |
| --- | --- | --- | --- |
| 测试工具 | 工具作用 | 工具版本 | 工具数量 |
| 华为云VSS | WEB扫描工具 | 最新版本 | 1 |
| RASA | 主机扫描工具 | 最新版本 | 1 |

## 3.2安全测试时间和测试人员

表格 2‑2安全测试时间和测试人员

|  |  |  |  |
| --- | --- | --- | --- |
| 开始时间 | 结束时间 | 测试描述 | 测试人员 |
| 2020/07/03 | 2020/07/07 | 对即将上线的商品智慧关务，按照华为云市场安全合规要求为主，产品已发现安全问题等为辅，通过安全工具和手工测试相结合进行验证 | XXX |

# 4测试执行

## 4.1安全测试结果综述及关键风险

### 4.1.1 产品安全红线总体达成目标

通过测试及检查，对即将上架中国区的智慧关务按照公司安全红线规定项目进行逐项核查

### 4.1.2 产品Web扫描高风险汇总和跟踪

|  |  |  |  |
| --- | --- | --- | --- |
| 问题描述 | 问题风险等级 | 处理结论 | 层面 |
| Redis 未授权访问漏洞  redis端口对外开放并且没有配置认证选项，未授权用户可直接获取数据库中所有信息，造成严重的信息泄露。 | 高 | 已按照修复建议修复 | Web |
| Redis配置不当可直接导致服务器被控制  redis端口对外开放并且没有配置认证选项，并且以root权限运行，未授权用户可直接覆盖/root/.ssh/authorized\_keys 上传公钥直接用root账号登陆ssh服务器。 | 高 | 已按照修复建议修复 | 服务器ip |

如果没有高危漏洞就删除表格

### 4.1.3 产品主机扫描高风险汇总和跟踪

|  |  |  |  |
| --- | --- | --- | --- |
| 问题描述 | 问题风险等级 | 处理结论 | 层面 |
| Redis 未授权访问漏洞  redis端口对外开放并且没有配置认证选项，未授权用户可直接获取数据库中所有信息，造成严重的信息泄露。 | 高 | 已按照修复建议修复 | Web |
| Redis配置不当可直接导致服务器被控制  redis端口对外开放并且没有配置认证选项，并且以root权限运行，未授权用户可直接覆盖/root/.ssh/authorized\_keys 上传公钥直接用root账号登陆ssh服务器。 | 高 | 已按照修复建议修复 | 服务器ip |

### 4.1.4 安全测试用例执行结果统计表

安全测试用例执行结果分成三级：

**发现问题**:测试过程中发现的问题

**遗留问题**: 测试完成后未得到解决或确认为风险比较低或者不强制要求修改的问题

**已解决问题：**确认为工具误报或已经修复的问题

表格 3‑3-1安全测试结果统计表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 分类 | 高危漏洞 | 中危漏洞 | 低危漏洞 | 已解决问题 | 遗留问题 | 测试人员 |
| 系统组件安全 | 0 | 2 | 9 | 0 | 11 | xxx |
| 第三方组件安全 |
| 系统安全配置 | 0 | 0 | 0 | 0 | 0 |
| Web安全配置 | 0 | 0 | 13 | 0 | 13 |
| 合计 | 0 | 2 | 22 | 0 | 24 |

说明：

Web扫描：总共发现xxx个高危漏洞，xxx个中级漏洞，xxx个低级漏洞，经xxx轮修复，剩余xxx个中危漏洞，xxx个低危漏洞，风险均可接受风险

主机扫描：总共发现xxx个高危漏洞，xxx个中级漏洞，xxx个低级漏洞，经xxx轮修复，剩余xxx个中危漏洞，xxx个低危漏洞，风险均可接受风险

### 4.1.5防暴力破解机制检测



说明：网页登录设置了输入多次错误密码被锁定的方式，存在防暴力破解机制，符合鲲鹏认证测试规范。（次数限制，图片验证，短信验证等。）

# 5安全测试记录

## 5.1安全测试日志

1. * + 1. 操作系统扫描报告



* + - 1. Web扫描报告



# 6安全测试总结

## 6.1测试总结

遵循安全合规的要求，结合扫描工具评分的结果，经总体评估该平台安全风险较低。

## 6.2结果确认

|  |  |
| --- | --- |
| 被测试方：重庆超体科技有限公司 | 测试方：鲲鹏计算产业生态重庆中心 |
| 测试人员签名：XXX | 测试人员签名：xxx |
| 时间：2020-07-07 | 时间：2020-07-07 |