UiBot RPA 平台

安全测试报告

北京来也网络科技有限公司

目录

1、综述

本次评估采用单节点部署方案进行安全测试，系统安全评估系统从如下几个方面进行分类统计：

- 业务安全漏洞列表
- 主机系统安全漏洞列表
- 数据库配置安全漏洞列表
- 脆弱账号安全漏洞列表

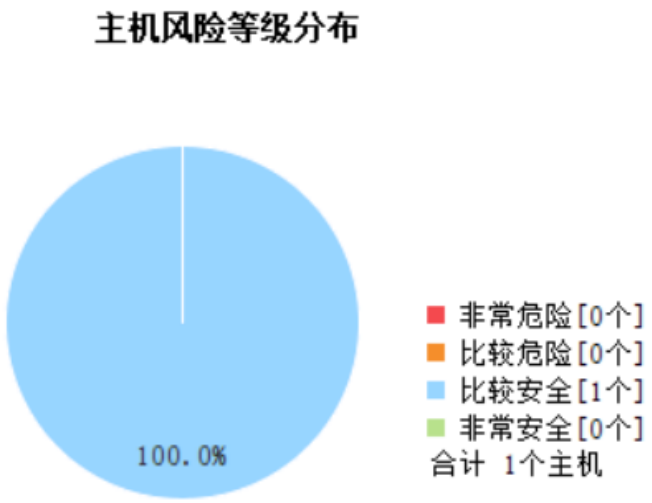
系统安全等级为比较安全，其中有 6 个主机系统安全等级为比较危险。具体评估标准请查看底部安全评测标准。

1.1 任务信息

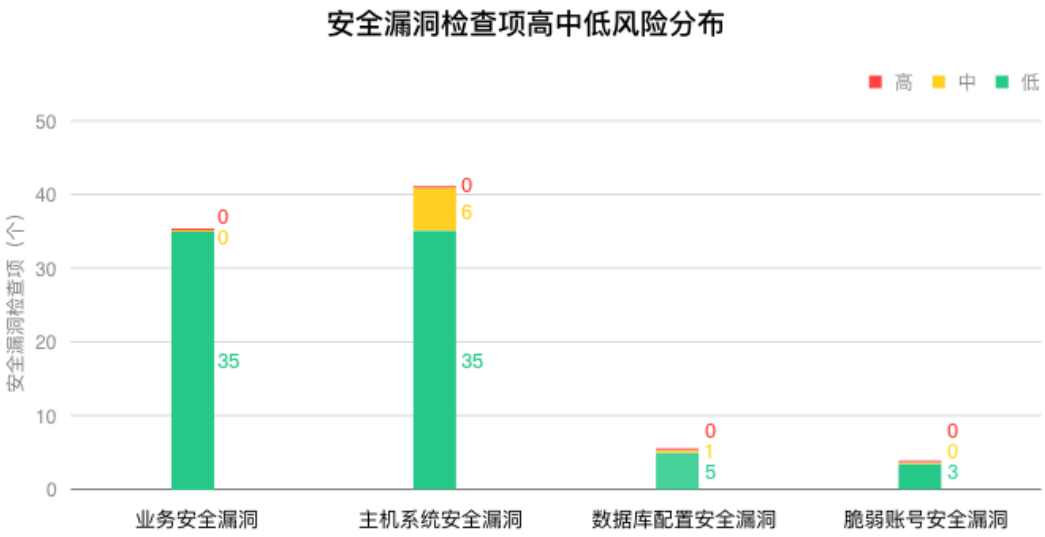
任务名称	Commander 5.3.0 私有部署安全检查
风险评估	比较安全
任务类型	安全评估
存活主机	1
成功扫描主机	1
失败扫描主机	0
未扫描主机	0
开始时间	2020-11-18
结束时间	2020-11-18

1.2 风险分布

1.2.1 主机风险分布



1.2.2 风险分布总览



1.3 资产综述

操作系统	主机数量	比率
Centos7	1	100%
合计	1	100%

2、风险分布

2.1 漏洞风险类别

2.1.1 业务安全漏洞

检查项		描述	风险值
域名安全	域名管理漏洞	检查域名管理账号或邮箱是否安全，域名是否可被劫持。	0
业务安全	弱密码漏洞	检查系统是否使用策略来强制限制密码长度和复杂性。	0
	业务逻辑漏洞	检查系统业务流程处理，查看是否存在逻辑不严谨导致的安全隐患。 1、对数据包进行签名校验，防止数据包在传输的过程中被篡改。 2、用户操作均在服务端进行校验，而不是简单的通过 JS 进行校验。 3、重要功能增加确认操作或重新认证。 4、在每个会话中使用强随机令牌（token）来保护。 5、验证一切来自客户端的参数，重点是和权限相关的参数。	0
	业务越权漏洞	检查系统对用户访问角色的权限是否进行严格的检查及限制，不存在低权用户操作高权业务，当前账号操作其他账号业务权限。	0
代码漏洞	SQL 注入漏洞	对系统各功能参数进行注入测试，查看是否存在 SQL 注入漏洞。	0
	XSS 跨站漏洞	对核心业务 HTTP 请求中的各参数进行 XSS 验证。	0
	OS 命令注入	检查系统是否存在命令注入漏洞。	0
	XXE 注入漏洞	检查系统是否存在 XML 外部实体注入漏洞。	1

	任意文件读取漏洞	检查系统资源调用模块是否存在文件非法读取漏洞、文件包含漏洞。	0
	任意文件上传漏洞	检查网站文件上传写入模块是否允许向服务器写入 WEBSHELL 文件。	0
	任意文件修改删除漏洞	检查文件编辑模块是否存在删除、修改任意文件的问题。	0
	URL 跳转漏洞	检查网站是否存在 URL 跳转漏洞。	0
	访问控制漏洞	检查系统各个模块用户权限控制问题，是否存在模块越权访问、访问控制缺失等问题。	0
	身份认证漏洞	检查用户认证方式是否安全，登陆口令是否可被爆破。	0
	会话管理漏洞	检查系统会话管理方式是否安全，是否存在固定会话、SESSIONID 泄露、登陆超时、COOKIE 错误使用等问题。	0
	敏感注释信息或代码泄露	检查系统代码注释中是否包含敏感信息或测试代码。	3
	第三方组件漏洞	检查系统是否使用了不安全的第三方组件。	2
防护策略	HTTP 请求签名	检查系统是否对请求进行防篡改签名，签名是否可被绕过。	0
	应用防火墙规则绕过	检查防火墙防护能力，安全策略是否生效，策略是否可以绕过。	0
	应用防火墙防护绕过	检查是否可通过直接访问系统 IP 等方式绕过安全防护。	0
中间件配置	错误页面自定义	检查系统是否自定义错误页面。	0
	控制台弱口令或漏洞	检查中间件控制台是否弱口令或存在漏洞。	0
	目录及其他错误配置	检查中间件配置是否合规。	3
	危险的 HTTP 方法	检查中间件是否开启危险的 HTTP 方法。	0
数据库安全	数据库允许远程连接	检查数据库端口是否对外开放，是否允许远程连接。	0
	数据库补丁更新不及时	检查数据库是否存在已知漏洞。	1
通信安全	HTTPS 明文传输	检查是否使用 HTTPS 加密传输。	0
	HTTPS 证书未校验漏洞	检查 HTTPS 证书是否校验。	0
	Get 方式传输关键参数	检查系统关键参数是否使用安全的 post 方式传输。	0
	HTTPS 中间人攻击漏洞	检查系统数据传输是否存在中间人劫持风险。	0
信息泄露	敏感文件泄露	检查系统目录中是否存在系统备份文件、说明文件、缓存文件、测试文件等，导致系统源码、配置信息泄露。	0

	后台地址泄露	检查系统租户路径是否进行隐藏。	0
服务器安全	非业务端口开放	检查系统是否开放危险的非业务端口开放。	0
	服务补丁检查器	检查服务器是否及时更新补丁，是否存在可利用高危漏洞。	0
	远程管理口令安全	检查远程管理软件口令策略是否安全，是否存在弱口令、口令爆破问题。	1

2.1.2 主机系统安全漏洞

序号	漏洞名称	影响主机个数	风险值
1	CentOS Oracle MySQL Server 安全漏洞(CVE-2019-2529)	1	0
2	CentOS ISC BIND 安全限制绕过漏洞(CVE-2018-5741)	1	0
3	CentOS Oracle MySQL Server 组件访问控制错误漏洞	1	5
4	CentOS Oracle MySQL/MariaDB 组件安全漏洞(CVE-2018-3282)	1	0
5	CentOS Oracle MySQL Server 安全漏洞(CVE-2019-2503)	1	0
6	CentOS Polkit polkitd 信息泄露漏洞(CVE-2018-1116)	1	5
7	CentOS grub2 输入验证错误漏洞(CVE-2020-14311)	1	0
8	CentOS grub2 输入验证错误漏洞(CVE-2020-14310)	1	0
9	CentOS Linux kernel 信息泄露漏洞(CVE-2018-16658)	1	0
10	CentOS dbus 授权问题漏洞(CVE-2019-12749)	1	0
11	CentOS ISC BIND 远程拒绝服务漏洞(CVE-2018-5745)	1	0
12	CentOS Oracle MySQL Server 访问控制错误漏洞	1	0
13	CentOS Linux kernel 信息泄露安全漏洞(CVE-2019-3460)	1	5
14	CentOS Linux kernel 信息泄露安全漏洞(CVE-2019-3459)	1	5
15	CentOS Apple iOS libxml2 内存破坏漏洞(CVE-2015-8035)	1	5
16	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)【原理扫描】	1	0
17	CentOS Linux kernel 安全漏洞(CVE-2018-15594)	1	5
18	CentOS Linux kernel 安全漏洞(CVE-2018-7755)	1	0
19	CentOS Linux kernel 信息泄露漏洞(CVE-2019-7222)	1	0
20	CentOS 多款 Intel 产品安全漏洞(CVE-2020-0543)	1	0
21	CentOS 多款 Intel 产品信息泄露漏洞(CVE-2020-0548)	1	0
22	CentOS 多款 Intel 产品信息泄露漏洞(CVE-2020-0549)	1	0
23	CentOS Linux kernel 数字错误漏洞(CVE-2018-13053)	1	0
24	CentOS Linux kernel 缓冲区错误漏洞(CVE-2018-19985)	1	0
25	CentOS Linux kernel 输入验证错误漏洞(CVE-2019-17055)	1	0
26	CentOS systemd-journald 缓冲区错误漏洞(CVE-2018-16866)	1	0
27	CentOS Linux kernel 安全漏洞(CVE-2019-19338)	1	0
28	CentOS Info-ZIP UnZip 资源管理错误漏洞(CVE-2019-13232)	1	0
29	CentOS Linux kernel 命令注入漏洞(CVE-2019-11884)	1	0
30	CentOS Linux kernel 代码问题漏洞(CVE-2019-10207)	1	0
31	CentOS Linux Kernel 本地信息泄露漏洞(CVE-2019-11833)	1	0
32	CentOS Linux kernel 安全漏洞(CVE-2019-5489)	1	0

33	CentOS 多款 Intel 产品安全漏洞(CVE-2019-0154)	1	0
34	CentOS Linux Kernel 本地拒绝服务漏洞(CVE-2017-17807)	1	0
35	CentOS systemd 安全漏洞(CVE-2018-16888)	1	0
36	CentOS Libgcrypt 安全漏洞(CVE-2018-0495)	1	0
37	CentOS Linux kernel 信息泄露漏洞(CVE-2019-18660)	1	0
38	通过 SSH 检测到主机使用的 DNS 服务器地址	1	0
39	探测到 SSH 服务器支持的算法	1	0
40	SSH 版本信息可被获取	1	0
41	检测到 Linux/UNIX 系统信息	1	0

2.1.3 数据库配置安全漏洞

检查配置项	漏洞描述	影响主机数	风险值
其他安全	检查是否存在空密码	1	0
账号口令	检查是否更改默认 MYSQL 管理员账号	1	0
其它安全	检查是否根据机器性能和业务需求，设置最大连接数	1	0
文件安全	检查是否禁止 MYSQL 对本地文件存取	1	0
日志审计	检查是否配置日志功能	1	4

2.1.4 脆弱账号安全漏洞

类别	描述	影响主机	风险值
业务系统脆弱账号	1、检查是否存在空密码。 2、检查是否使用策略来强制限制密码长度和复杂性。 3、检查是否更改默认密码。	1	0
服务器脆弱账号	1、检查是否存在空密码。 2、检查是否使用策略来强制限制密码长度和复杂性。 3、检查是否更改默认密码。	1	0
数据库脆弱账号	1、检查是否存在空密码。 2、检查是否使用策略来强制限制密码长度和复杂性。 3、检查是否更改默认密码。	1	0

3.参考标准

3.1 漏洞风险等级评估标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <= 10	攻击者可以远程执行任意命令或者代码，对系统行远程拒绝服务攻击。
中	4 <= 漏洞风险值 < 7	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
低	0 <= 漏洞风险值 < 4	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。

3.2 配置检查项风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 检查项风险值 <= 10	不当的配置导致攻击者可以通过其他方式获得管理员权限、或者只有管理员权限才能加固的配置。
中	4 <= 检查项风险值 < 7	不当的配置导致攻击者可以对主机进行破坏或者收集主机的信息、或者遭受攻击后，重要事件没有记录。
低	0 <= 检查项风险值 < 4	不当地配置对主机安全不会造成太大的影响。

3.3 主机风险等级评定标准

主机风险等级	主机风险值区域
非常危险	7.0 <= 主机风险值 <= 10.0
比较危险	5.0 <= 主机风险值 < 7.0
比较安全	2.0 <= 主机风险值 < 5.0
非常安全	0.0 <= 主机风险值 < 2.0

说明：

1、按照安全评估系统的主机风险评估模型计算主机风险值。根据得到的主机风险值参考“主机风险等级评定标准”标识主机风险等级。

2、将主机风险等级按照风险值的高低进行排序，得到非常危险、比较危险、比较安全、非常安全四种主机风险等级。

3.4 网络风险等级评定标准

网络风险等级	网络风险值区域
非常危险	8.0 <= 网络风险值 <= 10.0
比较危险	5.0 <= 网络风险值 < 8.0
比较安全	1.0 <= 网络风险值 < 5.0
非常安全	0.0 <= 网络风险值 < 1.0

说明：

1、按照安全评估系统的网络风险评估模型计算该网络风险值。根据得到的网络风险值参考“网络风险等级评定标准“标识网络风险等级。

2、将网络风险等级按照风险值的高低进行排序，得到非常危险、比较危险、比较安全、非常安全四种网络风险等级。

3.5 安全建议

据市场研究报告称"实施漏洞管理的企业会避免近 90%的攻击"。可以看出，及时的漏洞修补可以 在一定程度上防止病毒、攻击者的威胁。

1、建议所有 Windows 系统使用"Windows Update"进行更新。

2、对于大量终端用户而言，可以采用 WSUS 进行自动补丁更新，也可以采用补丁分发系统及时对终端用户进行补丁更新。

3、对于存在弱口令的系统，需在加强使用者安全意识的前提下，督促其修改密码，或者使用策略来强制限制密码长度和复杂性。

4、对于存在弱口令或是空口令的服务，在一些关键服务上，应加强口令强度，同时需使用加密传输方式，对于一些 可关闭的服务来说，建议关闭该服务以达到安全目的。

5、对于 UNIX 系统订阅厂商的安全公告，与厂商技术人员确认后进行漏洞修补、补丁安装、停止服务等。

6、由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。

7、建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，攻与防的循环，伴随每个主流操作系统、应用服务的生命周期。

8、建议采用安全评估系统定期对网络进行评估，真正做到未雨绸缪。远程安全评估系统建议对存在不合规检查项的主机参考对应的检查点详情中提出的调整方案和标准值进行修正。