

|  |  |  |  |
| --- | --- | --- | --- |
| 安全评估报告 | | | |
| ■ 文档编号 |  | ■ 密级 | 商业机密 |
| ■ 版本编号 | V1.0 | ■ 日期 | 2022-02-07 |



|  |
| --- |
| © 2022 青藤云安全 |

|  |
| --- |
| ■ 版权声明 |
| 本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**青藤云安全**所有，受到有关产权及版权法保护。任何个人、机构未经**青藤云安全**的书面授权许可，不得以任何方式复制或引用本文的任何片断。 |

|  |  |  |  |
| --- | --- | --- | --- |
| ■ 版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
| 2022-02-07 | V1.0 | 文档创建 | 安全交付中心 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| ■ 适用性声明 |
| 本文档为北京升鑫网络科技有限公司（以下简称“青藤云安全”）对公司（以下简称“”）进行青藤云安全产品正式部署后输出的安全评估分析报告，适用于相关技术人员对发现的安全风险进行修复时参考。 |

**目录**

[一. 概述 1](#_Toc535951661)

[1.1 评估人员 1](#_Toc535951662)

[1.2 评估时间 1](#_Toc535951663)

[1.3 评估范围 2](#_Toc535951664)

[1.4 安全评估内容 2](#_Toc535951665)

[1.5 资产清点 2](#_Toc535951666)

[**1.5.1** **操作系统分布情况** 2](#_Toc535951673)

[**1.5.2** **Agent在线率** 2](#_Toc535951674)

[二. 安全评估结果摘要 3](#_Toc535951675)

[三. 安全评估结果分析 3](#_Toc535951676)

[3.1 安全评估问题分布 3](#_Toc535951677)

[3.2 风险发现 3](#_Toc535951678)

[3.2.1 Linux漏洞风险 3](#_Toc535951679)

[3.2.2 Linux弱密码 5](#_Toc535951680)

[3.2.3 Linux 应用漏洞 12](#_Toc535951681)

[3.2.4 Windows弱密码 15](#_Toc535951682)

[3.3 入侵检测 15](#_Toc535951683)

[**3.3.1** **系统后门** 15](#_Toc535951684)

[**3.3.2** **Web后门** 17](#_Toc535951685)

[四. 总结 18](#_Toc535951686)

[附录A 单一漏洞危险等级评定标准 20](#_Toc535951687)

[附录B 主机风险等级评定标准 21](#_Toc535951688)

[附录C 网络风险等级评定标准 22](#_Toc535951689)

# 概述

安全评估主要是通过青藤云安全对评估范围内的服务器和网络、安全设备进行安全扫描，对被评估对象进行一系列的安全分析与探测，以发现目标存在的安全隐患并确实的告知修复建议，是安全体系搭建工作中修复安全风险，提升安全等级的重要工作之一。

通过安全评估工作，可以详细的了解当前网络和系统中存在的潜在安全隐患，有效发现网络设备、操作系统和应用软件在用户帐号、口令、安全漏洞、服务配置等方面存在的安全风险、漏洞和威胁，同时梳理安全修复工作，以危害程度高低划分修复工作，阶段性的提供有效、明确的修复方案，为进一步通过技术手段降低或解决发现的问题提供了参考依据和方法。

在安全评估项目中，青藤云安全使用自适应安全系统对系统进行了安全评估，通过对结果的分析，对目前存在的安全风险以危害程度进行划分，针对目前危害程度最高的风险提供了建议解决方案，供相关人员参考。

## 评估人员

表1.1.1评估人员

|  |  |  |
| --- | --- | --- |
| **姓名** | **所属部门** | **邮箱** |
|  | 安全交付中心 |  |

## 评估时间

表1.2.1评估时间

|  |  |
| --- | --- |
| **评估时间** | |
| **起始时间** | 2022-02-07 |
| **结束时间** | 2022-02-07 |

## 评估范围

本次安全评估范围为青藤服务器与在线的30台主机。

## 安全评估内容

本次安全评估内容包括下内容：

* 获取安全评估范围内设备系统和应用版本等信息；
* 评估安全评估范围内的系统、服务和应用的帐号、口令的安全状况；
* 评估安全评估范围内的系统、应用漏洞情况；
* 评估安全评估范围内的系统被入侵情况；

## 资产清点

* + 1. **操作系统分布情况**

本次扫描共发现114台主机，操作系统分布如下表：

表1.5.1.1 操作系统分布表

|  |  |
| --- | --- |
| 漏洞名称 | **主机数** |
| CentOS Linux release 7.9.2009 (Core) | 19 |
| CentOS Linux release 7.6.1810 (Core) | 15 |
| CentOS Linux release 7.5.1804 (Core) | 10 |
| CentOS Linux release 7.7.1908 (Core) | 8 |
| CentOS Linux release 7.4.1708 (Core) | 8 |
| CentOS release 6.5 (Final) | 5 |
| CentOS Linux release 7.8.2003 (Core) | 2 |
| CentOS Linux release 8.5.2111 | 2 |
| Kylin Linux Advanced Server release V10 (Sword) | 1 |
| CentOS release 6.8 (Final) | 1 |
| CentOS Linux release 8.2.2004 (Core) | 1 |
| CentOS Linux release 7.9.2009 (AltArch) | 1 |
| Ubuntu 16.04.5 LTS (Xenial Xerus) | 1 |
| Ubuntu 20.04 LTS (Focal Fossa) | 1 |
| CentOS release 6.9 (Final) | 1 |
| Ubuntu 18.04.5 LTS (Bionic Beaver) | 1 |
| Kali GNU/Linux 2020.1 | 1 |
| Windows 10 Education (build 16299) | 3 |
| Windows 7 Ultimate Service Pack 1 (build 7601) | 3 |
| Windows 10 Pro (build 10240) | 2 |
| Windows Server 2008 R2 Datacenter Service Pack 1 (build 7601) | 2 |
| Windows Server 2016 Standard (build 14393) | 2 |
| Windows Server 2016 Datacenter (build 14393) | 2 |
| Microsoft Windows Server 2016 Datacenter (build 14393) | 2 |
| Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 (build 7601) | 2 |
| Microsoft Windows 11 专业版 (build 22000) | 1 |
| Windows 10 Education (build 18363) | 1 |
| Windows 10 Pro (build 18363) | 1 |
| Microsoft Windows 7 Home Basic Service Pack 1 (build 7601) | 1 |
| Microsoft Windows Server 2012 R2 Standard (build 9600) | 1 |
| Microsoft Windows 10 家庭中文版 (build 19043) | 1 |
| Microsoft Windows 10 家庭中文版 (build 19042) | 1 |
| Windows Server 2012 Standard (build 9200) | 1 |
| Windows 10 Home China (build 19042) | 1 |
| Windows 10 Pro (build 19042) | 1 |
| Microsoft Windows 7 专业版 Service Pack 1 (build 7601) | 1 |
| Microsoft Windows Server 2008 HPC Edition Service Pack 1 (build 7601) | 1 |
| Microsoft Windows Server 2016 Standard (build 14393) | 1 |
| Windows 10 Home (build 19044) | 1 |
| Windows 10 Education (build 17134) | 1 |
| Windows Server 2012 R2 Standard (build 9600) | 1 |
| Windows 7 Enterprise Service Pack 1 (build 7601) | 1 |
| Windows Server 2008 R2 Standard Service Pack 1 (build 7601) | 1 |
| Windows Server 2019 Standard (build 17763) | 1 |

* + 1. **Agent在线率**

本次扫描发现114台主机安装agent，其中30台在线，84台离线。在线率：26.31%

# 安全评估结果摘要

本次安全巡检主要对应用风险，系统风险，账号风险，弱密码，系统漏洞，入侵诊断5方面进行安全巡检，摘要如下：

1. 发现10个推荐优先修复漏洞，已给出主机IP、漏洞简介、修复建议。
2. 发现121个应用弱口令账号，已给出主机IP、账号。
3. 发现10项高危应用风险，已给出优先修复问题主机IP，修复建议。
4. 发现4项高危系统风险，已给出优先修复问题主机IP，修复建议。
5. 发现7项高危账号风险，已给出优先修复问题主机IP，修复建议。

# 安全评估结果分析

## 安全评估问题分布

安全评估问题分布从资产清点、风险发现、入侵检测3大项来进行安全评估安全风险，排查系统中存在的应用弱密码、高危漏洞、Web后门文件、系统后门文件、系统权限设置等风险项。

## 风险发现

### Linux漏洞风险

3.2.1.1漏洞补丁情况

|  |  |  |  |
| --- | --- | --- | --- |
| 漏洞名称 | **影响IP** | **漏洞类型** | **危险程度** |
| Apache Log4j 远程代码执行漏洞(CVE-2021-44228、CVE-2021-45046) | 4台 | 代码执行 | 危急 |
| Linux polkit本地权限提升漏洞(CVE-2021-4034) | 17台 | 本地提权 | 高危 |
| Atlassian Confluence 远程代码执行漏洞(CVE-2020-4027) | 1台 | 代码执行 | 中危 |
| Shiro RememberMe 1.2.4 反序列化过程命令执行漏洞(CVE-2016-4437) | 2台 | 不安全的反序列 | 高危 |
| Tomcat存在文件包含漏洞(CVE-2020-1938) | 2台 | 任意文件读取 | 高危 |
| Bash环境变量远程命令执行漏洞(CVE-2014-6271) | 1台 | 命令执行 | 危急 |
| Struts2 S2-059 远程代码执行漏洞(CVE-2019-0230) | 1台 | 代码执行 | 高危 |
| glibc幽灵漏洞(CVE-2015-0235) | 1台 | 命令执行 | 危急 |
| Struts2 S2-057 远程代码执行漏洞(CVE-2018-11776) | 1台 | 代码执行 | 危急 |
| glibc缓冲区溢出漏洞(CVE-2014-5119) | 1台 | 代码执行 | 高危 |

表 3.2.1.2 漏洞补丁分析及建议

|  |  |  |
| --- | --- | --- |
| **漏洞名称** | **影响IP** | **漏洞描述&修复建议** |
| Apache Log4j 远程代码执行漏洞(CVE-2021-44228、CVE-2021-45046) | 4台 | Apache Log4j是一个功能强大的日志组件，提供方便的日志记录。  Apache Log4j2存在远程代码执行漏洞，由于Apache Log4j2某些功能存在递归解析功能，攻击者可直接构造恶意请求，触发远程代码执行漏洞。 【修复建议】1.Java 6 将 log4j 升级到 2.3.1 版本，Java 7 将 log4j 升级到 2.12.3 版本，Java 8 或更高版本将 log4j 升级到 2.17.0 版本，下载地址：https://logging.apache.org/log4j/2.x/download.html  2.若暂时无法升级，删除jar包中漏洞相关的JndiLookup.class文件： zip -q -d log4j-core-xxx.jar org/apache/logging/log4j/core/lookup/JndiLookup.class 【修复影响】服务重启 |
| Linux polkit本地权限提升漏洞(CVE-2021-4034) | 17台 | polkit是一个在类 Unix操作系统中控制系统范围权限的组件。通过定义和审核权限规则，实现不同优先级进程间的通讯。  polkit存在本地权限提升漏洞，由于pkexec无法正确处理调用参数计数，攻击者可利用该漏洞通过精心设计环境变量诱导pkexec执行任意代码，具有低权限的攻击者可以利用此漏洞绕过pkexec自带的安全保护措施，获取目标机器的ROOT权限。 【修复建议】将漏洞检测结果中的软件包升级到对应漏洞修复版本及以上，补丁修复可能存在docker网络断开风险，修复需谨慎，建议测试验证无误后进行升级操作。  参照安全补丁功能中该漏洞的修复命令进行升级，或者参照以下修复命令进行升级：  CentOS/RedHat/Oracle Linux : sudo yum update -y 需要升级的软件包名(参考检测结果)  SUSE : sudo zypper update -y 需要升级的软件包名(参考检测结果)  Ubuntu/Debian : sudo apt-get update && sudo apt-get install --only-upgrade -y 需要升级的软件包名(参考检测结果)  例：若漏洞的检测结果中主机系统为 CentOS 7，软件包名称为 polkit，当前安装版本为 0.112-26.el7，对应漏洞修复版本为 0.112-26.el7\_9.1，则漏洞修复命令为 sudo yum update -y polkit 【修复影响】服务重启 |
| Atlassian Confluence 远程代码执行漏洞(CVE-2020-4027) | 1台 | Atlassian Confluence是一个专业的企业知识管理与协同软件。  Atlassian Confluence存在漏洞，该漏洞允许具有系统管理权限的远程攻击者通过自定义用户宏中的注入漏洞绕过速度模板注入缓解措施，造成任意远程代码执行。 【修复建议】将 Confluence 升级到 7.4.4，7.5.1及以上版本，下载地址：https://www.atlassian.com/software/confluence/download 【修复影响】服务重启 |
| Shiro RememberMe 1.2.4 反序列化过程命令执行漏洞(CVE-2016-4437) | 2台 | Apache Shiro是一个强大且易用的Java安全框架，执行身份验证、授权、密码学和会话管理。使用Shiro的易于理解的API，您可以快速、轻松地获得任何应用程序，从最小的移动应用程序到最大的网络和企业应用程序。  Shiro默认使用了CookieRememberMeManager，其处理Cookie的流程是：得到rememberMe的cookie值–>Base64解码–>AES解密–>反序列化。然而AES的密钥是硬编码的Base64.decode(“kPH+bIxk5D2deZiIxcaaaA==”) ，加解密算法是CBC并且初始化向量IV未被真正使用就导致了攻击者可以构造恶意数据造成反序列化的RCE漏洞。 【修复建议】将 Shiro 升级到 1.2.5、2.0.0 及以上版本，下载地址：http://shiro.apache.org/download.html 【修复影响】不需要重启 |
| Tomcat存在文件包含漏洞(CVE-2020-1938) | 2台 | Tomcat 服务器是一个免费的开放源代码的Web 应用服务器，属于轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用，是开发和调试JSP 程序的首选。  Tomcat中存在文件包含漏洞，该漏洞由于Tomcat AJP协议存在实现缺陷导致相关参数可控，攻击者利用该漏洞可通过构造特定参数，读取服务器webapp下的任意文件。若目标服务器AJP端口对外开放（默认为8009端口），且同时存在文件上传功能，攻击者可进一步实现远程代码的执行。 【修复建议】将 Tomcat 升级到 7.0.100、8.5.51、9.0.31 及以上版本，下载地址：http://archive.apache.org/dist/tomcat/ 【修复影响】服务重启 |
| Bash环境变量远程命令执行漏洞(CVE-2014-6271) | 1台 | Shellshock，又称Bashdoor，是在Unix中广泛使用的Bash shell中的一个安全漏洞，首次于2014年9月24日公开。许多互联网守护进程，如网页服务器，使用bash来处理某些命令，从而允许攻击者在易受攻击的Bash版本上执行任意代码。这可使攻击者在未授权的情况下访问计算机系统。该漏洞会影响目前主流的Linux和Mac OSX操作系统平台，包括但不限于Redhat、CentOS、Ubuntu、Debian、Fedora、Amazon Linux、OS X 10.10等平台。 【修复建议】将漏洞检测结果中的软件包升级到对应漏洞修复版本及以上。  参照安全补丁功能中该漏洞的修复命令进行升级，或者参照以下修复命令进行升级：  CentOS/RHEL/Oracle Linux : sudo yum update -y 需要升级的软件包名(参考检测结果)  SUSE : sudo zypper update -y 需要升级的软件包名(参考检测结果)  Ubuntu/Debian : sudo apt-get update && sudo apt-get install --only-upgrade -y 需要升级的软件包名(参考检测结果)  例：若漏洞的检测结果中主机系统为 SUSE 11，软件包名称为 libreadline5，当前安装版本为 5.2-11.22.1，对应漏洞修复版本为 5.2-147.22.1，则漏洞修复命令为 sudo zypper update -y libreadline5 【修复影响】系统重启 |
| Struts2 S2-059 远程代码执行漏洞(CVE-2019-0230) | 1台 | Apache Struts2是一款用于创建企业级Java Web应用的开源框架。Struts2在使用某些tag等情况下可能存在OGNL表达式注入漏洞，从而导致远程代码执行。 【修复建议】将 Struts2 升级到 2.5.22 及以上版本，下载地址：https://struts.apache.org/download 【修复影响】服务重启 |
| glibc幽灵漏洞(CVE-2015-0235) | 1台 | GHOST漏洞是glibc库中的\_\_nss\_hostname\_digits\_dots()函数中存在一个缓冲区溢出漏洞，这个bug可以经过gethostbyname\*()函数被本地或者远程的触发。应用程序主要使用gethostbyname\*()函数发起DNS请求，这个函数会将主机名称转换为ip地址。这个名为幽灵（GHOST）的高危安全漏洞出现在2015年，可以允许攻击者远程获取操作系统的最高控制权限，影响市面上大量Linux操作系统及其发行版。 【修复建议】将漏洞检测结果中的软件包升级到对应漏洞修复版本及以上。  参照安全补丁功能中该漏洞的修复命令进行升级，或者参照以下修复命令进行升级：  CentOS/RHEL/Oracle Linux : sudo yum update -y 需要升级的软件包名(参考检测结果)  SUSE : sudo zypper update -y 需要升级的软件包名(参考检测结果)  Ubuntu/Debian : sudo apt-get update && sudo apt-get install --only-upgrade -y 需要升级的软件包名(参考检测结果)  例：若漏洞的检测结果中主机系统为 SUSE 11，软件包名称为 glibc-devel，当前安装版本为 2.1.3-17.74.13，对应漏洞修复版本为 2.11.3-17.74.13，则漏洞修复命令为 sudo zypper update -y glibc-devel 【修复影响】不需要重启 |
| Struts2 S2-057 远程代码执行漏洞(CVE-2018-11776) | 1台 | Struts2 中存在远程代码执行漏洞，当上层操作配置没有namespace或通配符配置namespace时，如果基础xml配置中未设置namespace值或者使用没有value和action设置的url标签，可能导致远程代码执行。 【修复建议】将 Struts2 升级到 2.3.35、2.5.17 及以上版本，下载地址：https://struts.apache.org/download 【修复影响】服务重启 |
| glibc缓冲区溢出漏洞(CVE-2014-5119) | 1台 | glibc包提供标准的C库(libc)，POSIX线程库(libpthread)，标准数学库(libm)和系统上多个程序使用的名称服务缓存守护程序(nscd)。 没有这些库，Linux系统无法正常运行。  glibc中的\_\_gconv\_translit\_find()函数存在基于堆的缓冲区溢出漏洞。攻击者能够使应用程序通过特制参数调用iconv\_open()函数，利用该漏洞以该应用程序的权限执行任意代码。 【修复建议】将漏洞检测结果中的软件包升级到对应漏洞修复版本及以上。  参照安全补丁功能中该漏洞的修复命令进行升级，或者参照以下修复命令进行升级：  CentOS/RHEL/Oracle Linux : sudo yum update -y 需要升级的软件包名(参考检测结果)  SUSE : sudo zypper update -y 需要升级的软件包名(参考检测结果)  Ubuntu/Debian : sudo apt-get update && sudo apt-get install --only-upgrade -y 需要升级的软件包名(参考检测结果)  例：若漏洞的检测结果中主机系统为 ubuntu 14.04，软件包名称为libc6，当前安装版本为 2.11-0ubuntu6.3，对应漏洞修复版本为 2.19-0ubuntu6.3，则漏洞修复命令为sudo apt-get update && sudo apt-get install --only-upgrade -y libc6 【修复影响】不需要重启 |

### Linux弱密码

* + - 1. MySQL弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 主机IP | 端口 | 账号名 | 密码值 | 弱密码类型 |
| 10.0.8.9 | 3306 | nan | \*\* | 空密码 |
| 10.0.8.9 | 3306 | nan | \*\* | 空密码 |
| 172.17.56.226 | 3306 | nan | \*\* | 空密码 |
| 172.17.56.226 | 3306 | nan | \*\* | 空密码 |
| 172.17.56.226 | 3306 | newGw | roo\*\*\* | 常见弱密码 |
| 172.17.56.226 | 3306 | newGw | roo\*\*\* | 常见弱密码 |
| 192.168.192.230 | 3306 | root | 123\*\*\* | 常见弱密码 |
| 192.168.192.230 | 3306 | root | 123\*\*\* | 常见弱密码 |
| 192.168.192.230 | 3306 | root | 123\*\*\* | 常见弱密码 |
| 10.0.0.32 | 3306 | root | \*\* | 空密码 |
| 10.0.0.32 | 3306 | root | \*\* | 空密码 |
| 10.0.0.32 | 3306 | nan | \*\* | 空密码 |
| 10.0.0.32 | 3306 | nan | \*\* | 空密码 |
| 10.0.0.32 | 3306 | confluence | con\*\*\* | 密码与用户名相同 |
| 10.0.0.32 | 3306 | confluence | con\*\*\* | 密码与用户名相同 |

* + - 1. SSH弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 主机IP | 账号名 | 登录方式 | 密码值 | 弱密码类型 |
| 192.168.192.74 | root | 密码登录 | Qin\*\*\* | 常见弱密码 |
| 192.168.192.232 | bigdata | 密码登录 | big\*\*\* | 密码与用户名相同 |
| 192.168.192.232 | root | 密码登录 | Qin\*\*\* | 常见弱密码 |
| 192.168.192.230 | gmq | 密码登录 | 123\*\*\* | 常见弱密码 |
| 192.168.192.230 | root | key或密码登录 | Qin\*\*\* | 常见弱密码 |
| 10.0.0.26 | qingteng | 密码登录 | qin\*\*\* | 密码与用户名相同 |
| 10.0.0.26 | trap | 密码登录 | tra\*\*\* | 常见弱密码 |

* + - 1. Redis弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 主机IP | 监听端口 | 绑定IP | 是否root权限 | 弱密码类型 |
| 192.168.192.230 | 6381 | 0.0.0.0 | 否 | 常见弱密码 |
| 192.168.192.230 | 6380 | 0.0.0.0 | 否 | 常见弱密码 |
| 192.168.192.230 | 6379 | 0.0.0.0 | 否 | 常见弱密码 |
| 192.168.192.85 | 6379 | 127.0.0.1 | 否 | 空密码 |

**修复建议：**

经检测发现上面列出的所有应用账号均存在弱口令问题。将帐户名与密码设置为相同属于弱口令。弱口令账号非常容易被攻破，一旦入侵者发现弱口令账号，可以在较短时间内攻破该账号，登录到应用，对系统产生更大危害。建议在不影响业务正常运转的情况下加强密码复杂度。

例如某些存在空口令问题的redis，同时可以被其他主机访问，启动权限为root，一旦黑客探测到redis服务，就相当于黑客有了root权限对系统任意位置写的能力，即可轻松远程植入木马或执行其他入侵操作。

以上弱口令问题均需为帐号加一个安全的口令。一个安全的口令应该包含以下四项中的三项：

（1）大写字母

（2）小写字母

（3）特殊字符

（4）数字

每种应用的弱密码修复示例，请见：“**附件-各应用弱密码常见修复方式示例.docx**” （该附件中提供的修复命令适用于相关技术人员进行风险修复时进行参考，修复弱密码时请您结合业务情况进行修复，建议优先在测试环境测试后，再通过同样的操作修复生产环境的漏洞。）

### Windows弱密码

1. Windows系统账户弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 主机IP | 弱密码帐户 | 账号状态 | 密码值 | 弱密码类型 |
| 172.24.231.10 | zouss | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhulp | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhuj | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhuhui | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhugn | 启用 | zhu\*\*\* | 密码与用户名相同 |
| 172.24.231.10 | zhuc | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhaowb | 启用 | 111\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhaos | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhaoa | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhangzb | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhangwenyuan | 启用 | aa1\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhangjh | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zhanghy | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | zangqt | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | yuhang | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | yuancq | 启用 | 543\*\*\* | 常见弱密码 |
| 172.24.231.10 | yaoyr | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | yanqian | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | yangxy | 启用 | 1\*\*\*\*\* | 常见弱密码 |
| 172.24.231.10 | xuzq | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | xujing | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | xucx | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | xiqn | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | xiangxj | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wush | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wujian | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wugl | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wug | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wufl | 启用 | 111\*\*\* | 常见弱密码 |
| 172.24.231.10 | wangyang | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wangsm | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wangrq | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wangpy | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wangjue | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wangjj | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | wangj | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | tuanwei | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | tuanw | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | tsn | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | tester | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | telephone | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | tangsn | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | sulg | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | shiyh | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | shenjiyh | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | shenjixt | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | shenjixg | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | shenjisy | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | shenjijk | 启用 | 123\*\*\* | 常见弱密码 |
| 172.24.231.10 | renwei | 启用 | 123\*\*\* | 常见弱密码 |
| ...完整弱密码列表请见：附件-弱密码列表-windwos |  |  |  |  |

安全建议：

经检测发现Windows上有主机存在弱口令问题。弱口令账号非常容易被攻破，一旦入侵者发现弱口令账号，可以在较短时间内攻破该账号，登录到系统，对系统产生较大危害。建议在不影响业务正常运转的情况下加强密码复杂度。

### 应用风险

表3.2.4.1 应用风险检查情况

|  |  |  |
| --- | --- | --- |
| 危险程度 | 风险名称 | 影响主机 |
| 高危 | MySQL服务存在默认test数据库 | 2台 |
| 高危 | Squid服务ACL安全配置检测 | 1台 |
| 高危 | Redis服务以root权限运行 | 1台 |
| 高危 | Tomcat服务存在example/docs样本应用 | 1台 |
| 高危 | Bind服务DNS递归查询配置检测 | 1台 |
| 高危 | Nginx host欺骗 | 1台 |
| 高危 | Redis服务存在CONFIG命令配置未被修改 | 1台 |
| 高危 | Tomcat运行权限检查 | 3台 |
| 高危 | Tomcat服务8005端口SHUTDOWN | 4台 |
| 高危 | NTP服务存在反射放大DOS攻击漏洞 | 2台 |

表3.2.4.1 应用风险检查情况详情

|  |  |  |
| --- | --- | --- |
| **漏洞名称** | **影响主机** | **漏洞描述&修复建议** |
| MySQL服务存在默认test数据库 | 2台 | MySQL中test数据库默认允许匿名用户访问，攻击者可通过该数据库进行数据库的敏感信息查询，造成敏感信息泄露。 【修复建议】删除test数据库  【修复影响】服务重启 |
| Squid服务ACL安全配置检测 | 1台 | /etc/squid/squid.conf中配置http\_access字段的值为 allow all 或http\_reply\_access字段的值为 allow all (允许所有人或客户端使用该代理) ，攻击者可通过squidclient执行相关mgr信息查询，导致squid服务器敏感信息泄露。 【修复建议】将/etc/squid/squid.conf配置文件http\_access allow all选项配置值all为允许指定网段。例:http\_access allow 192.168.8.0/24  【修复影响】服务重启 |
| Redis服务以root权限运行 | 1台 | Redis服务以root权限运行，攻击者可通过Redis对服务器文件进行任意操作或者执行命令。通过查询命令获取敏感信息，通过写入公钥信息获取ssh登录权限等。如果Redis为root权限，攻击者则无需提权直接对服务器进行操作。 【修复建议】备份数据（bgsave/save)后，在系统中新增加用户（useradd redis) 并给Redis数据文件赋予该新用户的权限，然后使用该新增加的用户（非root权限的用户）运行Redis，使得Redis启动后仍然可以从rdb或aof数据文件中快速建立缓存内容  【修复影响】服务重启 |
| Tomcat服务存在example/docs样本应用 | 1台 | Tomcat服务webapps中若存在example等类似默认样本应用，攻击者可利用example的漏洞入侵tomcat/docs，影响web服务器安全。 【修复建议】删除webapps文件夹中example、jsp-examples、examples、docs文件夹。  【修复影响】服务重启 |
| Bind服务DNS递归查询配置检测 | 1台 | 若该服务器为解析服务器，则不应该启用递归查询功能。如果DNS服务器允许递归解析到外网的设备，这一点可以被攻击者用来进行DNS放大攻击，即受害者将遭受攻击者的DDOS攻击。 【修复建议】在/etc/named.conf配置中，将allow-recursion配置项更改为allow-recursion { none; };或者将recursion配置项更改为recursion no;  【修复影响】服务重启 |
| Nginx host欺骗 | 1台 | 通常，位于Nginx后面的应用程序需要一个正确的主机头来生成URL（重定向，资源，邮件链接等）。  欺骗这个头，可能会导致从钓鱼到SSRF的各种问题。 【修复建议】1、在server name指令中列出所有正确的服务器名称，不使用变量;  2、总是使用$ host而不是$ http\_host。  【修复影响】服务重启 |
| Redis服务存在CONFIG命令配置未被修改 | 1台 | 若未修改/root/redis/redis.conf中默认的rename-command CONFIG设置项，攻击者可使用CONFIG命令对Redis的数据库文件位置进行修改和变更。通过在数据库中插入攻击者的ssh公钥信息，并执行bgsave命令可以将带有公钥信息的数据库文件写入被攻击者使用CONFIG命令指定的磁盘位置。CONFIG命令未做修改的情况下，攻击者可以很方便的完成这一攻击过程并最终获取操作系统权限。 【修复建议】将Redis配置文件中rename-command CONFIG 配置项更改为其他内容  【修复影响】服务重启 |
| Tomcat运行权限检查 | 3台 | 【漏洞描述】Tomcat以root权限运行时，应用程序（如Struts2、jsp webshell）也拥有了root权限，因此通过漏洞，可以直接以root用户身份控制主机。【修复建议】将tomcat运行账号切换至普通用户以及普通用户组【修复影响】服务重启 |
| Tomcat服务8005端口SHUTDOWN | 4台 | 该功能为Tomcat默认功能，TCP连接到Tomcat的默认8005端口，并输入"SHUTDOWN"即可关闭Tomcat。若生产环境未修改该指令，则可能导致任意关闭重要业务Tomcat服务。 【修复建议】修改配置文件/etc/tomcat6/server.xml默认端口号和SHUTDOWN关闭指令. 例:<Server port="端口号" shutdown="其它自定义命令">  【修复影响】服务重启 |
| NTP服务存在反射放大DOS攻击漏洞 | 2台 | NTP是用UDP传输的，所以可以伪造源地址并且在NTP协议中有一类查询指令，用短小的指令即可令服务器返回很长的信息。放大攻击就是基于这类指令的。网络上一般NTP服务器都有很大的带宽，攻击者可能只需要1Mbps的上传带宽欺骗NTP服务器，即可给目标服务器带来几百上千Mbps的攻击流量，从而造成拒绝服务攻击，如果攻击者同时向多台ntp服务器发送这种查询指令，则可以造成分布式拒绝服务攻击。 【修复建议】更新NTP版本到4.2.7p26以上，ntpd-4.2.7p26版本后，“monlist”特性已经被禁止，取而代之的是“mrulist”特性，使用mode6控制报文，并且实现了握手过程来阻止对第三方主机的放大攻击。  【修复影响】服务重启 |

### 系统风险

表3.2.5.1 系统风险检查情况

|  |  |  |
| --- | --- | --- |
| 危险程度 | 风险名称 | 影响主机 |
| 高危 | SSH支持存在安全漏洞的v1版本 | 2台 |
| 高危 | ldpreload存在可疑模块风险 | 3台 |
| 高危 | /var/spool/cron目录所有者、组所有者读写执行权限 | 3台 |
| 高危 | 路由转发功能开启 | 6台 |

表3.2.5.2系统风险检查情况详情

|  |  |  |
| --- | --- | --- |
| **漏洞名称** | **影响主机** | **漏洞描述&修复建议** |
| SSH支持存在安全漏洞的v1版本 | 2台 | SSH支持两种不同且不兼容的协议：SSH1和SSH2。 SSH1是原始协议，受到安全问题的约束。 SSH2更加先进和安全。 【修复建议】方法一： 手动添加Protocol 2 到/etc/ssh/sshd\_config文件中  方法二：在终端中执行下列命令：  sudo sed -i -e 's/#\*\(Protocol .\*\)/#\1/i' /etc/ssh/sshd\_config  echo 'Protocol 2' | sudo tee -a /etc/ssh/sshd\_config  【修复影响】服务重启 |
| ldpreload存在可疑模块风险 | 3台 | ldpreload用于动态库的加载，动态库加载的优先级最高，可以被用来在主程序和其动态链接库的中间加载别的动态链接库，甚至覆盖正常的函数库。 【修复建议】检测ldpreload设置的库文件是否为恶意，是否有过修改  【修复影响】不需要重启 |
| /var/spool/cron目录所有者、组所有者读写执行权限 | 3台 | 如果恶意用户拥有在/var/spool/cron目录创建一个文件的能力，他们可以轻松地在/var/spool/cron目录部署持久或预定恶意软件。/var/spool/cron目录应有700的目前权限。/var/spool/cron目录拥有者应该为root。/var/spool/cron应该具有root用户组所有权。 【修复建议】可执行如下命令进行修复：  chown root:root /var/spool/cron  chmod 700 /var/spool/cron  【修复影响】不需要重启 |
| 路由转发功能开启 | 6台 | 启用网络接口之间的数据包转发创建一个服务器的路由功能，该功能可以被滥用来创建或进一步的攻击，并能创造威胁的高度载体。如果这个检查失败，路由本身没有明确要求，把net.ipv4.ip\_forward的值更改为0来明确禁用IP路由。如果服务器有面向Internet和内部私人的两个接口，这一点就尤其重要。 【修复建议】1、永久修复方案(需重启系统后生效)：  对/etc/sysctl.conf手动配置net.ipv4.ip\_forward=0，  或复制和粘贴这些命令：  sudo sed -i -e 's/#\*\(net.ipv4.ip\_forward .\*\)/#\1/i' /etc/sysctl.conf  echo 'net.ipv4.ip\_forward = 0' | sudo tee -a /etc/sysctl.conf  2、临时修复方案  echo 0 > /proc/sys/net/ipv4/ip\_forward  【修复影响】不需要重启 |

### 账号风险

表3.2.6.1 账号风险检查情况

|  |  |  |
| --- | --- | --- |
| 危险程度 | 风险名称 | 影响主机 |
| 高危 | 账户目录任意读写 | 21台 |
| 高危 | 未设置密码复杂度限制 | 21台 |
| 高危 | 未设置密码尝试次数锁定 | 20台 |
| 高危 | 免密码可sudo的账号 | 9台 |
| 高危 | 账号未设置密码过期时间 | 21台 |
| 高危 | 账户密钥文件任意读写 | 5台 |
| 高危 | 非wheel组用户使用SU切换root | 21台 |

表3.2.6.2 账号风险检查情况详情

|  |  |  |
| --- | --- | --- |
| **漏洞名称** | **影响主机** | **漏洞描述&修复建议** |
| 账户目录任意读写 | 21台 | 用户账号目录可被任意读写，则意味着用户的变量信息或文件均可被任意改写，因此存在系统被提权或越权，或水坑攻击等风险。 【修复建议】修改用户账户目录的权限，某些应用可能对家目录权限有特殊要求，建议测试验证无误后再进行操作。  【修复影响】不需要重启 |
| 未设置密码复杂度限制 | 21台 | 用户可设置脆弱口令，从而使得攻击者有机会使用弱口令爆破的方式获得密码。 【修复建议】在配置文件中修改密码复杂度配置。例如/etc/pam.d/system-auth文件：password requisite pam\_cracklib.so minlen=8 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1  【修复影响】不需要重启 |
| 未设置密码尝试次数锁定 | 20台 | 攻击者可无限次尝试登录系统。 【修复建议】在上述文件中加入指定配置项，使用pam\_tally模块或pam\_faillock模块对登陆系统失败次数过多的账户进行锁定。  【修复影响】不需要重启 |
| 免密码可sudo的账号 | 9台 | 免密码可sudo账号往往存在一定的安全风险。 【修复建议】请删除免密码可sudo账号或者对该类账号添加强口令。  【修复影响】不需要重启 |
| 账号未设置密码过期时间 | 21台 | 用户账号密码应定期更换，若未设置密码过期时间，则用户可能不会有定期更换密码的意识，从而无法有效的保障账户安全。 【修复建议】将未设置过期时间的账户添加过期时间限制。  可以使用 chage -M [days] [username] 命令修改指定账号的密码过期时间。  【修复影响】不需要重启 |
| 账户密钥文件任意读写 | 5台 | 用户账号目录下的authorized\_keys文件权限不是标准的600，意味着用户的密钥可被其他用户读取或改写，因此存在系统被提权或越权，或水坑攻击等风险。 【修复建议】修改用户authorized\_keys文件权限为600： chmod 600 authorized\_keys  【修复影响】不需要重启 |
| 非wheel组用户使用SU切换root | 21台 | 任意用户如果获知root密码均可su到root用户。 【修复建议】在/etc/pam.d/su文件中增加auth required pam\_wheel.so use\_uid。  【修复影响】不需要重启 |

# 总结

为了保证系统的安全，青藤云安全评估小组通过专业的安全评估服务对应用系统进行了安全安全评估评估工作，通过这方面的工作可以及时检查出系统中存在的的高风险问题，从而极大地降低系统遭受攻击的可能性，提高应用系统的安全性。

通过安全评估可以部分主机存在高风险问题，建议尽早确认系统上残留的Web后门、系统后门，并清理和业务无关的高危可疑文件；建议尽快修复多数应用服务的弱口令问题；列出的危机漏洞已经是经过筛选后判断需要修复的漏洞，建议在不影响业务的情况下尽快修复。

1. 单一漏洞危险等级评定标准

|  |  |  |
| --- | --- | --- |
| **危险程度** | **危险值区域** | **危险程度说明** |
| 高 | 8 <= 漏洞风险值 <= 10 | 攻击者可以远程执行任意命令或者代码，或进行远程拒绝服务攻击。 |
| 中 | 5 <= 漏洞风险值 < 8 | 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 | 1 <= 漏洞风险值 < 5 | 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。 |

|  |  |
| --- | --- |
| **分值** | **评估标准** |
| 1 | 可远程获取OS、应用版本信息。 |
| 2 | 开放了不必要或危险的服务，可远程获取系统敏感信息。 |
| 3 | 可远程进行受限的文件、数据读取。 |
| 4 | 可远程进行重要或不受限文件、数据读取。 |
| 5 | 可远程进行受限文件、数据修改。 |
| 6 | 可远程进行受限重要文件、数据修改。 |
| 7 | 可远程进行不受限的重要文件、数据修改，或对普通服务进行拒绝服务攻击。 |
| 8 | 可远程以普通用户身份执行命令或进行系统、网络级的拒绝服务攻击。 |
| 9 | 可远程以管理用户身份执行命令（受限、不太容易利用）。 |
| 10 | 可远程以管理用户身份执行命令（不受限、容易利用）。 |

1. 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 <= 主机风险值 <= 10 |
| 比较危险 | 5 <= 主机风险值 < 7 |
| 比较安全 | 2 <= 主机风险值 < 5 |
| 非常安全 | 0 <= 主机风险值 < 2 |

1.将主机的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。

2.按照青藤云安全风险评估模型计算得到风险值。

注：高、中和低漏洞威胁的定义参见《单一漏洞威胁等级评定标准》

1. 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 <= 网络风险值 <= 10 |
| 比较危险 | 5 <= 网络风险值 < 8 |
| 比较安全 | 1 <= 网络风险值 < 5 |
| 非常安全 | 0 <= 网络风险值 < 1 |

网络风险等级是网络中所有主机威胁分值的加权平均和。

1 对网络中的所有主机按照威胁分值进行高低排序，依据主机的威胁分值将主机风险划分为高、中、低三个类别。

2.按照青藤云安全风险评估模型计算得到风险值。

其中：

非常危险的主机定义为高风险；比较危险的主机定义为中风险；比较安全和非常安全的主机定义为低风险。