

|  |  |  |  |
| --- | --- | --- | --- |
| $CName安全评估报告 | | | |
| ■ 文档编号 |  | ■ 密级 | 商业机密 |
| ■ 版本编号 | V1.0 | ■ 日期 | $Date |



|  |
| --- |
| © 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 |
| $Date | 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$CompanyName公司（以下简称“$CName”）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$CName安全评估项目中，青藤云安全使用自适应安全系统对$CName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** |
| $user\_name | 安全交付中心 | $user\_email\_name |

## 评估时间

表1.2.1评估时间

|  |  |
| --- | --- |
| **评估时间** | |
| **起始时间** | $Date |
| **结束时间** | $Date |

## 评估范围

本次安全评估范围为青藤服务器与在线的$count\_online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$count\_all台主机，操作系统分布如下表：

表1.5.1.1 操作系统分布表

|  |  |
| --- | --- |
| **$操作系统分布表** | **主机数** |
|  |  |

* + 1. **Agent在线率**

本次扫描发现$count\_all台主机安装agent，其中$count\_online台在线，$count\_offline台离线。在线率：$online\_rate%

# 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$vul\_count个推荐优先修复漏洞，已给出主机IP、漏洞简介、修复建议。
2. 发现$weak\_passwd\_count个应用弱口令账号，已给出主机IP、账号。
3. 发现$app\_vul\_count项高危应用风险，已给出优先修复问题主机IP，修复建议。
4. 发现$os\_vul\_count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$account \_vul\_count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

|  |  |  |  |
| --- | --- | --- | --- |
| **$Linux漏洞风险** | **影响IP** | **漏洞类型** | **危险程度** |
|  |  |  |  |

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** |
|  |  |  |

### Linux弱密码

* + - 1. MySQL弱密码问题列表$MySQL弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $MySQL弱密码问题列表 | 端口 | 账号名 | 密码值 | 弱密码类型 |
|  |  |  |  |  |

* + - 1. SSH弱密码问题列表$SSH弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $SSH弱密码问题列表 | 账号名 | 登录方式 | 密码值 | 弱密码类型 |
|  |  |  |  |  |

* + - 1. Redis弱密码问题列表$Redis弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $Redis弱密码问题列表 | 监听端口 | 绑定IP | 是否root权限 | 弱密码类型 |
|  |  |  |  |  |

* + - 1. Tomcat弱密码问题列表$Tomcat弱密码问题列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| $Tomcat弱密码问题列表 | 账号状态 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |  |

* + - 1. Rsync弱密码问题列表$Rsync弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $Rsync弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. Weblogic弱密码问题列表$Weblogic弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $Weblogic弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. Jenkins弱密码问题列表$Jenkins弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $Jenkins弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. OpenLDAP弱密码问题列表$OpenLDAP弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $OpenLDAP弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. InfluxDB弱密码问题列表$InfluxDB弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $InfluxDB弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. ProFTPD弱密码问题列表$ProFTPD弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $ProFTPD弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. SVN弱密码问题列表$SVN弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $SVN弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. PPTP弱密码问题列表$PPTP弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $PPTP弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. VNC弱密码问题列表$VNC弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $VNC弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. OpenVPN弱密码问题列表$OpenVPN弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $OpenVPN弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

* + - 1. vsftpd弱密码问题列表$vsftpd弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $vsftpd弱密码问题列表 | 账号名 | 密码值 | 弱密码类型 | 监听端口 |
|  |  |  |  |  |

**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$windows系统账户弱密码问题列表

1. Windows系统账户弱密码问题列表$windows系统账户弱密码问题列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $windows系统账户弱密码问题列表 | 弱密码帐户 | 账号状态 | 密码值 | 弱密码类型 |
|  |  |  |  |  |

**安全建议：$windows系统账户弱密码问题列表**

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。$windows系统账户弱密码问题列表

### 应用风险$应用风险检查情况

表3.2.4.1 应用风险检查情况$应用风险检查情况

|  |  |  |
| --- | --- | --- |
| $应用风险检查情况 | 风险名称 | 影响主机 |
|  |  |  |

表3.2.4.1 应用风险检查情况详情$应用风险检查情况

|  |  |  |
| --- | --- | --- |
| **漏洞名称** | **影响主机** | **漏洞描述&修复建议** |
|  |  |  |

### 系统风险$系统风险检查情况

表3.2.5.1 系统风险检查情况$系统风险检查情况

|  |  |  |
| --- | --- | --- |
| $系统风险检查情况 | 风险名称 | 影响主机 |
|  |  |  |

表3.2.5.2系统风险检查情况详情$系统风险检查情况

|  |  |  |
| --- | --- | --- |
| **漏洞名称** | **影响主机** | **漏洞描述&修复建议** |
|  |  |  |

### 账号风险$账号风险检查情况

表3.2.6.1 账号风险检查情况$账号风险检查情况

|  |  |  |
| --- | --- | --- |
| $账号风险检查情况 | 风险名称 | 影响主机 |
|  |  |  |

表3.2.6.2 账号风险检查情况详情$账号风险检查情况

|  |  |  |
| --- | --- | --- |
| **漏洞名称** | **影响主机** | **漏洞描述&修复建议** |
|  |  |  |

# 总结

为了保证$CName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。