

青藤云安全

风险发现-弱密码常见修复方法示例

让安全更有效

二零二二年二月

|  |
| --- |
| ■ 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 |
| 2022-02-04 | V3.4.0.8 | 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有限公司（以下简称“青藤云安全”）的风险发现-弱密码常见修复方法示例，适用于相关技术人员进行风险修复时进行参考。**本文所提供的所有操作，请您务必在确认不会对业务产生影响的情况下执行**，建议您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。 |

目 录

[ **Weblogic** 2](#_Toc94904333)

[ **Jenkins** 3](#_Toc94904334)

[ **Tomcat** 4](#_Toc94904335)

[ **OpenLDAP** 4](#_Toc94904336)

[ **InfluxDB** 6](#_Toc94904337)

[ **ProFTPD** 6](#_Toc94904338)

[ **SVN** 7](#_Toc94904339)

[ **MySQL** 7](#_Toc94904340)

[ **PPTP** 8](#_Toc94904341)

[ **VNC** 9](#_Toc94904342)

[ **SSH** 10](#_Toc94904343)

[ **OpenVPN** 11](#_Toc94904344)

[ **rsync** 11](#_Toc94904345)

[ **Redis** 12](#_Toc94904346)

[ **vsftpd** 13](#_Toc94904347)

* **Weblogic**

**【应用介绍】**

WebLogic是用于开发、集成、部署和管理大型分布式Web应用、网络应用和数据库应用的Java应用服务器。

**【风险描述】**

Weblogic中的弱密码被爆破成功后，入侵者可以：

* 对配置文件、机密信息和其他资产随意进行增删查改
* 窃取/泄露/传播机密信息、利用服务器内信息绑架勒索等不法行为
* 提权执行更高权限操作，包括控制服务器
* 安装木马或病毒等破坏服务器安全性的脚本程序

**【修复方法】**

**一、Console可登陆：**

1. 登陆后进入“域结构-安全领域”(Domain Structure-Security Realms）
2. 点击右侧的myrealm
3. 选择标签“用户和组”（Users and Groups），在下方找到要修改的用户名
4. 选择标签“密码”(Passwords)
5. 输入两次密码后点击save即修改完成

该方法不需要重启服务

**二、命令行修改密码**

1. 进入域目录

cd /home/weblogic/bea/user\_projects/domains/{your domain name}/servers/AdminServers/security

或

cd $BEA\_BASE/user\_projects/domains/{your domain name}/servers/AdminServer/security/

1. 修改boot.properties里的username和password

cat boot.properties

1. 完成后保存配置并重启weblogic服务

# 关闭weblogic服务

ps -ef|grep weblogic

kill -9 {id}

# 启动并挂载weblogic

nohup ./startWebLogic.sh &

* **Jenkins**

**【应用介绍】**

Jenkins是一个独立的开源软件项目，是基于Java开发的一种持续集成工具，用于监控持续重复的工作，旨在提供一个开放易用的软件平台，使软件的持续集成变成可能。

**【风险描述】**

Jenkins被爆破成功后，入侵者可以：

* 直接获取、修改、删除所有账户已部署的源代码和其他资产
* 窃取/泄露/传播机密信息、利用源码绑架勒索等不法行为
* 进一步提权执行更高权限操作，甚至进一步控制服务器
* 安装后门、木马其他高危程序

**【修复方法】**

**一、可视化控制台修改**

1. 登陆Jenkins，点击左侧系统管理
2. 找到管理用户
3. 在用户列表页面找到要修改的用户，点击右侧的修改图标
4. 在用户详细页面底部找到修改密码，点击应用和Save
5. 注销用户并重新登陆

**二、命令行修改密码**

1. 使用在线工具生成一个Bcrypt密码 [Bcrypt密码生成器](https://www.jisuan.mobi/p163u3BN66Hm6JWx.html) (输入原密码和Rounds)后保存下来并记住原密码
2. 进入JENKINS\_HOME（Jenkins应用目录）/users，进入要修改的用户文件夹
3. 打开文件config.xml，找到<passwordHash>节点

vim config.xml

1. 将<passwordHash>节点内容改为

<**passwordHash**>jbcrypt:{生成的Bcrypt密码}</**passwordHash**>

<!--例如密码111111对应修改：-->

<**passwordHash**>jbcrypt:$2a$10$DdaWzN64JgUtLdvxWIflcuQu2fgrrMSAMabF5TSrGK5nXitqK9ZMS</**passwordHash**>

1. 保存并重启Jenkins应用

service jenkins restart

1. 重新登陆，输入用户名和新密码即可登陆

* **Tomcat**

**【应用介绍】**

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。

**【风险描述】**

Tomcat被爆破成功后，入侵者可以：

* 篡改配置文件、端口、内存和其他信息
* 窃取/泄露/传播机密信息、利用信息进行绑架勒索等不法行为
* 提权执行更高权限操作，甚至获取服务器控制权
* 安装木马或病毒等破坏服务器安全性的脚本程序

**【修复方法】**

1. 进入tomcat目录下，修改文件/conf/tomcat-users.xml

vim /conf/tomcat-users.xml

1. 找到待修改的用户名及对应密码，如：

<**role** rolename="admin-gui"/>

<**role** rolename="manager-gui"/>

<**user** username="root" password="[新的复杂密码]" roles="admin-gui,manager-gui"/>

1. 修改后重启Tomcat，以新密码登陆

* **OpenLDAP**

**【应用介绍】**

OpenLDAP是轻型目录访问协议（Lightweight Directory Access Protocol，LDAP）的自由和开源的实现，在其OpenLDAP许可证下发行，并已经被包含在众多流行的Linux发行版中。

**【风险描述】**

OpenLDAP被爆破成功后，入侵者可能：

* 篡改或伪造配置文件、加密证书等重要信息
* 根据目录快速窃取/泄露/传播机密敏感信息、利用信息进行绑架勒索

**【修复方法】**

1. 使用ldapsearch命令查询管理员的dn

ldapsearch -H ldapi:// -LLL -Q -Y EXTERNAL -b “cn=config” “(olcRootDN=\*)” dn olcRootDN olcRootPW

# 记住返回结果中的{dn}

1. 使用slappasswd生成密码

slappasswd -s [新的复杂密码]

# 记住返回结果中的{SSHA}密码

1. 使用ldapmodify修改条目

ldapmodify -Y EXTERNAL -H ldapi: ///

1. 输入修改的条目信息

dn: olcDatabase={2}bdb,cn=config #这是之前获取的管理员dn

replace: olcRootPW

olcRootPW: {SSHA}vAYFH48G4IfrpD57gTR/DNZqLHWzR+Fg #这里之前生成的密码{SSHA}

输入完毕按Ctrl+D退出交互模式

1. 出现modifying entry "olcDatabase={2}bdb,cn=config”说明修改成功
2. 重启slapd

/etc/init.d /slapd restart

* **InfluxDB**

**【应用介绍】**

InfluxDB 是一个开源分布式时序、事件和指标数据库。使用 Go 语言编写，无需外部依赖。其设计目标是实现分布式和水平伸缩扩展。

**【风险描述】**

InfluxDB被爆破成功后，入侵者可以：

* 窃取/泄露/传播数据库数据，利用信息进行绑架勒索
* 提权执行更高权限操作，对数据库甚至服务器进行随意篡改

**【修复方法】**

1. 登陆InfluxDB控制台

influx -username -password

1. 执行语句修改密码

SET PASSWORD FOR [要修改密码的用户名] = '[新的复杂密码]'

1. 重新登陆验证是否修改成功

* **ProFTPD**

**【应用介绍】**

ProFTPD是Unix平台上或类Unix平台上（如Linux, FreeBSD等）的FTP服务器程序。

**【风险描述】**

ProFTPD被爆破成功后，入侵者可以：

* 窃取/泄露/传播机密文件，利用文件进行绑架勒索
* 提权执行更高权限操作，甚至获得服务器控制权限

**【修复方法】**

1. 默认情况下，ProFTPD使用服务器系统用户，以root登陆修改密码即可

passwd [待修改的用户名]

1. 如果找不到用户名，尝试以下语句导入用户

useradd -c '[用户名]' -d /path/to/ftp/folder -s /sbin/nologin

仍无法解决建议使用pam模块，过程较为复杂，详见官方文档： <http://www.proftpd.org/docs/howto/Authentication.html>

* **SVN**

**【应用介绍】**

*SVN*是subversion的缩写，是一个开放源代码的版本控制系统，通过采用分支管理系统的高效管理，简而言之就是用于多个人共同开发同一个项目，实现共享资源，实现最终集中式的管理。

**【风险描述】**

SVN被爆破成功后，入侵者可以：

* 直接获取、修改、删除账户下的源代码和其他资产
* 窃取/泄露/传播源代码、利用源码绑架勒索等不法行为
* 代码中嵌入木马、病毒或其他高危程序

**【修复方法】** **一、临时修改密码**

svn up --username [待修改的用户名] --password [新的复杂密码]

**二、永久切换**

删除目录subversion/auth下所有文件后重新登陆

cd .subversion/auth

rm -rf\*

* **MySQL**

**【应用介绍】**

MySQL是一种开源的关系型数据库管理系统（RDBMS），使用最常用的数据库管理语言--结构化查询语言SQL进行数据库管理。

**【风险描述】**

MySQL被爆破成功后，入侵者可以：

* 窃取/泄露/传播数据库数据，利用数据进行绑架勒索
* 提权执行更高权限操作，对数据库进行随意增删查改

**【修复方法】**

**一、在mysqladmin中**

输入命令后提示输入原密码，正确后即可修改

mysqladmin -u[用户名] -p[旧密码] PASSWORD [新密码]

**二、Mysql host用户名查询及修改**

1. 以root身份进入mysql并输入密码

mysql -u root -p [原密码]

1. 查询数据库中所有用户的Host、User、Password信息

use [数据库名称]

SELECT host,user,password FROM user

1. 修改密码

UPDATE user SET password=PASSWORD("[新密码]") WHERE host='[用户名对应host]' AND User='[用户名]';

# 例如：

UPDATE user SET password=PASSWORD("12345") WHERE host='localhost' AND User='root';

若报错执行下列语句 update user SET authentication\_string=password('[新密码]') WHERE Host='[用户名对应host]' AND User='[用户名]';

1. 刷新退出

flush privileges;

exit;

tips：如果出现空账号，请删除该账号即可，这个为高危配置，必须处理；

delete from mysql.user where user='';

flush privileges;

* **PPTP**

**【应用介绍】**

PPTP(Point to Point Tunneling Protocol)，即点对点隧道协议。该bai协议是在PPP协议的基础上开发的一种新的增强型安全协议，支持多协议虚拟专用网(VPN)，可以通过密码验证协议(PAP)、可扩展认证协议(EAP)等方法增强安全性。

**【风险描述】**

PPTP被爆破成功后，如果未限制固定ip连接，入侵者可以：

* 获取虚拟专用网络的访问权限，冒用伪造身份进行隧道通信
* 如果被侵入设备已连接内网，则可以直接窃取/泄露/传播内网资源

**【修复方法】**

1. 修改配置文件

vi /etc/ppp/chap-secrets

1. 在文件中找到账户并修改密码（用户名与options.pptpd中对应）

# 用户名 服务器 密码 IP 地址

[待修改用户名] pptpd [原密码] \*

1. 保存退出

:wq!

* **VNC**

**【应用介绍】**

VNC (Virtual Network Console)是虚拟网络控制台的缩写。它 是一款优秀的远程控制工具软件，由著名的 AT&T 的欧洲研究实验室开发的。

**【风险描述】**

VNC被爆破成功后，入侵者可以：

* 远程控制账户所绑定的任意跨平台设备
* 窃取/泄露/传播远程设备上的数据，利用数据进行绑架勒索
* 提权执行更高权限操作，随意修改、删除设备文件或资源

**【修复方法】**

**一、忘记VNC密码重置**

1. 暂停VNC服务

stop vncserver

1. 删除root用户的VNC密码

rm -rf /root/.vnc/passwd

1. 启动VNC服务并重新设置密码

vncserver

1. 根据提示输入两次新密码即可

**！注意**：输入两次密码后出现提示”Would you like to enter a view-only password (y/n)? “（您想设定仅限查看的密码吗？）

请输入N不设置，设置该密码可能导致连接VNC出现黑屏的情况

**二、修改不同登陆系统身份的VNC密码**

1. 以对应身份登入系统或使用su切换用户
2. 修改当前用户启动vnc的密码

vncpasswd root

1. 根据提示输入两次新密码即可

**！注意**：输入两次密码后出现提示”Would you like to enter a view-only password (y/n)? “（您想设定仅限查看的密码吗？）

请输入N不设置，设置该密码可能导致连接VNC出现黑屏的情况

* **SSH**

**【应用介绍】**

SSH 为 Secure Shell 的缩写，由 IETF 的网络小组（Network Working Group）所制定；SSH 为建立在应用层基础上的安全协议。SSH 是较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

**【风险描述】**

SSH被爆破成功后（未设置SSH2密钥），入侵者可以：

* 远程连接服务器，获得服务器控制权
* 篡改配置文件、端口、内存和其他信息
* 窃取/泄露/传播机密信息、利用信息进行绑架勒索等不法行为
* 安装木马、病毒或后门等破坏服务器安全性的脚本程序

**【修复方法】**

1. 登陆服务器直接执行passwd

passwd [待修改的用户名]

1. 输入两次新密码即可

* **OpenVPN**

**【应用介绍】**

OpenVPN 是一个基于 OpenSSL 库的应用层 VPN 实现。和传统 VPN 相比，它的优点是简单易用。

**【风险描述】**

OpenVPN被爆破成功后，入侵者可以：

* 获取虚拟专用网络的访问权限，冒用伪造身份进行通信
* 如果被侵入设备已连接内网，则可以直接窃取/泄露/传播/破坏内网资源

**【修复方法】**

1. 在OpenSSL中添加或更改密码：

openssl rsa -**in** client.key -out client2.key -des3

1. 根据提示输入当前密码，再输入新密码即可

* **rsync**

**【应用介绍】**

rsync是linux系统下的数据镜像备份工具。使用快速增量备份工具Remote Sync可以远程同步，支持本地复制，或者与其他SSH、rsync主机同步。

**【风险描述】**

rsync被爆破成功后（未使用证书或开启免密登陆），入侵者可以：

* 直接获取已生成的目录树和文件系统镜像
* 窃取/泄露/传播数据文件、利用这些文件进行绑架勒索等不法行为
* 利用同步安装木马或病毒等破坏安全性的脚本程序

**【修复方法】**

1. 修改rsync deamon配置文件

vim /etc/rsyncd.conf

1. 找到secrets file修改为如下内容

secrets file = /etc/rsync.password #对应的密码文件

1. 生成该密码文件

echo "rsync\_backup:[新的复杂密码]">/etc/rsync.password

chmod 600 /etc/rsync.password # 权限

1. 写入密码文件

cat /etc/rsync.password

rsync\_backup:[新的复杂密码]

* **Redis**

**【应用介绍】**

Redis（Remote Dictionary Server )，即远程字典服务，是一个开源的使用ANSI C语言编写、支持网络、可基于内存亦可持久化的日志型、Key-Value数据库，并提供多种语言的API。

**【风险描述】**

redis被爆破成功后，入侵者可以:

* 窃取/泄露/传播数据库数据，利用数据进行绑架勒索
* 提权执行更高权限操作，对数据库进行随意增删查改

**【修复方法】**

**一、命令行修改密码**

1. 登入redis控制台

redis-cli -p [端口号](默认为6379)

1. 查看当前是否有密码

config get requirepass

1. 设置密码

config set requirepass [新的复杂密码]

1. 重新登录

redis-cli -h [host地址] -p [端口号] -a [新密码]

**二、修改配置文件**

1. 进入配置文件

vim /etc/redis.conf

1. 找到requirepass，如有注释则去除，修改为

requirepass [新的复杂密码]

1. 保存后重启redis服务

service redis stop

service redis start

* **vsftpd**

**【应用介绍】**

vsftpd（very secure FTP daemon） 是一个 UNIX 类操作系统上运行的服务器的名字，它可以运行在诸如 Linux、BSD、Solaris、 HP-UNIX等系统上面，是一个完全免费的、开放源代码的ftp服务器软件

**【风险描述】**

vsftpd被爆破成功后，入侵者可以：

* 窃取/泄露/传播机密文件，利用文件进行绑架勒索
* 提权执行更高权限操作，甚至获得服务器控制权限

**【修复方法】**

1. 登陆服务器进入应用根目录

cd /etc/vsftpd

1. 查看ftp用户名列表

cat ftpusers

1. 修改指定用户名的密码

passwd [待修改用户名]

1. 跟随指引输入密码后，重启vsftpd

service vsftpd restart

* **PostgreSQL**

**【应用介绍】**

PostgreSQL是以加州大学伯克利分校计算机系开发的 POSTGRES，现在已经更名为PostgreSQL，版本 4.2为基础的对象关系型数据库管理系统（ORDBMS）。PostgreSQL支持大部分 SQL标准并且提供了许多其他现代特性：复杂查询、外键、触发器、视图、事务完整性、MVCC。

**【风险描述】**

用户存在弱口令黑客可登录数据库进行脱库等操作。

**【修复方法】**

登入数据库，然后执行：

ALTER USER [弱密码用户名] with password ‘[新的复杂密码]’