Memcached服务安全加固

# 漏洞描述：

Memcached是一套常用的key-value缓存系统，由于它本身没有权限控制模块，所以开放在外网的Memcache服务很容易被攻击者扫描发现，通过命令交互可直接读取memcache中的敏感信息。

# 修复方案：

因Memcached无权限控制功能，所以需要用户对访问来源进行限制。

以下为具体的Memached 服务加固方案：

## 1.配置访问控制

建议用户不要讲服务发布到互联网上被黑客利用，可以通过[ECS安全组规则](https://help.aliyun.com/document_detail/25475.html?spm=5176.doc25470.6.204.SlE11A)或iptables配置访问控制规则。

iptables -A INPUT -p tcp -s 192.168.0.2 —dport 11211 -j ACCEPT

上述规则的意思是只允许192.168.0.2这个ip对11211端口进行访问。

## 2.—bind 制定监听IP

如果Memcached没有在外网开放的必要，可在Memcached启动的时候指定绑定的ip地址为 127.0.0.1。例如：

1. memcached -d -m 1024 -u memcached -l 127.0.0.1 -p 11211 -c 1024 -P /tmp/memcached.pid

## 3.最小化权限运行

使用普通权限账号运行，以下指定memcached 用户运行

1. memcached -d -m 1024 -u memcached -l 127.0.0.1 -p 11211 -c 1024 -P /tmp/memcached.pid

## 4.修改默认端口

修改默认11211监听端口为11222端口：

1. memcached -d -m 1024 -u memcached -l 127.0.0.1 -p 11222 -c 1024 -P /tmp/memcached.pid

参数说明：

-d选项是启动一个守护进程；

-m是分配给Memcached使用的内存数量，单位是MB，以上为1024MB；

-u是运行Memcached的用户，推荐单独普通权限用户：memcached，不要使用root权限账户；

-l是监听的服务器IP地址我这里指定了服务器的IP地址x.x.x.x；

-p是设置Memcached监听的端口，这里设置了11211，建议设置1024以上的端口；

-c选项是最大运行的并发连接数，默认是1024，这里设置了512，按照您服务器的负载量来设定；

-P是设置保存Memcached的pid文件，这里是保存在 /tmp/memcached.pid；

## 5.备份数据

为避免数丢失，升级前请做好备份，或ECS建立硬盘快照。