MapReduce 服务

服务公告

文档版本 01

发布日期 2023-12-12

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 漏洞公告

1.1 Apache Log4j2 远程代码执行漏洞（CVE-2021-44228）修复指导

本章节指导用户修复log4j2的CVE-2021-44228漏洞。目前有两种方式可以采用如下两种方式修复：

- 现有集群节点安装补丁
- 扩容节点安装补丁

前提条件

- 从OBS路径中下载的补丁工具“MRS_Log4j_Patch.tar.gz”。
- 确认集群主OMS节点：

  说明

  OMS节点一般为Master1和Master2节点，主OMS节点判断方法，执行以下命令，返回结果为active的节点为主OMS节点，返回结果为standby的节点为备OMS节点：

  3.x之前版本：

  sh /opt/Bigdata/*/workspace0/ha/module/hacom/script/get_harole.sh

  3.x及之后版本：

  sh /opt/Bigdata/om-server*/OMS/workspace0/ha/module/hacom/script/get_harole.sh

现有集群节点安装补丁

步骤1 将“MRS_Log4j_Patch.tar.gz”上传至主OMS节点的“/home/omm”目录下。具体可参考**如何上传本地文件到集群内节点？**。

步骤2 使用**root**用户登录主OMS节点，修改补丁工具相应权限，切到**omm**用户下，并解压补丁工具至当前目录。

chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz

su - omm

cd /home/omm

tar -zxf MRS_Log4j_Patch.tar.gz

步骤3 在“/home/omm/MRS_Log4j_Patch/bin/ips.ini”文件中配置需要打补丁的节点IP（当前集群所有节点IP）。

说明

每行配置一个IP，中间不能有空行。

步骤4 执行脚本安装补丁。

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh upgrade &

通过**tail -f nohup.out**可查看执行情况（打印 “upgrade patch success.” 表示执行完成）。

步骤5 登录Manager页面，重启受影响的组件，受影响组件请参考**受影响组件列表**。建议业务低峰期时执行重启操作。

步骤6 （可选）如果要新下载的客户端安装上补丁，需要先为部件包安装补丁，可执行如下命令：

su - omm

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh upgrade_package &

通过**tail -f nohup.out**查看执行情况，打印“upgrade_package patch success.”表示执行完成。

执行完之后，重新下载的客户端就已经是安装补丁的客户端。

注意

该步骤耗时比较长，且执行完之后不需要重启组件。

----结束

扩容节点安装补丁

步骤1 扩容操作时关闭“启动组件”开关。

步骤2 将“MRS_Log4j_Patch.tar.gz”上传至主OMS节点的“/home/omm”目录下。具体可参考**如何上传本地文件到集群内节点?** 。

步骤3 使用**root**用户登录主OMS节点，修改补丁工具相应权限，切到**omm**用户下，并解压补丁工具至当前目录。

chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz

su - omm

cd /home/omm

tar -zxf MRS_Log4j_Patch.tar.gz

步骤4 在“/home/omm/MRS_Log4j_Patch/bin/ips.ini”文件中配置需要打补丁的节点IP（当前集群扩容节点IP）。

说明

每行配置一个IP，中间不能有空行。

步骤5 执行脚本安装补丁。

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh upgrade &

通过**tail -f nohup.out**可查看执行情况，打印“upgrade patch success.”表示执行完成。

步骤6 登录Manager页面，启动新扩容节点上的实例。

----结束

补丁卸载方法

步骤1 使用**root**用户登录主OMS节点，执行如下命令，卸载脚本：

su - omm

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh rollback &

通过**tail -f nohup.out**可查看执行情况，打印“rollback patch success.”表示执行完成。

步骤2 登录Manager页面，重启受影响的组件，受影响组件请参考**受影响组件列表**。建议业务低峰期时执行重启操作。

步骤3 如果安装补丁时执行了**现有集群节点安装补丁**的**步骤6**，且希望回退部件包中的修改，可在**步骤2**执行完之后执行如下操作：

使用**root**用户登录主OMS节点，执行如下命令：

su - omm

cd /home/omm/MRS_Log4j_Patch/bin

nohup sh install.sh rollback_package &

通过**tail -f nohup.out**查看执行情况（打印“rollback_package patch success.”表示执行完成）。

----结束

ECS 重置密码插件升级（可选）

华为云ECS服务提供了一键式重置密码功能，弹性云服务器的密码丢失或过期时，可使用该功能进行一键式重置密码。重置密码插件为ECS内部运行的客户端进程，不对外提供任何网络服务，重置密码插件CloudResetPwdUpdateAgent使用了Apache Log4j2组件，经华为云安全实验室分析验证，ECS重置密码插件无可利用条件，无安全风险。

如果用户需要升级该插件中的Log4j2版本，可通过下面的步骤升级插件：

步骤1 将“MRS_Log4j_Patch.tar.gz”上传至主OMS节点的“/home/omm”目录下。具体可参考**如何上传本地文件到集群内节点?** 。

步骤2 使用**root**用户登录主OMS节点，修改补丁工具相应权限，切到**omm**用户下，并解压补丁工具至当前目录。

chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz

su - omm

cd /home/omm

tar -zxf MRS_Log4j_Patch.tar.gz

步骤3 在“/home/omm/MRS_Log4j_Patch/bin/ips.ini”文件中配置需要打补丁的节点IP（当前集群所有节点IP）。

说明

每行配置一个IP，中间不能有空行。

步骤4 根据节点登录方式执行以下步骤：

- **密码登录**

  执行以下命令：

  nohup sh install.sh upgrade_resetpwdagent passwd:*登录密码* &

  例如密码为xyz123，则命令为：

  nohup sh install.sh upgrade_resetpwdagent passwd:xyz123 &

  通过**tail -f nohup.out**查看执行情况，打印“upgrade_resetpwdagent patch success.”表示执行完成。

- **密钥登录**

  a. 将root用户对应的私钥文件上传到“/home/omm/MRS_Log4j_Patch/bin”目录下，保证文件的属组为root:root，执行命令：

  chown root:root /home/omm/MRS_Log4j_Patch/bin/*密钥文件*

  chmod 644 /home/omm/MRS_Log4j_Patch/bin/*密钥文件*

  b. 执行以下命令

  su - omm

  cd /home/omm/MRS_Log4j_Patch/bin

  nohup sh install.sh upgrade_resetpwdagent privatekey:*私钥文件路径* &

  例如私钥文件路径为‘/home/omm/MRS_Log4j_Patch/bin/abc.pem’，则执行命令为：

  nohup sh install.sh upgrade_resetpwdagent privatekey:/home/omm/MRS_Log4j_Patch/bin/abc.pem &

  通过**tail -f nohup.out**查看执行情况，打印“upgrade_resetpwdagent patch success.”表示执行完成。

----结束

受影响组件列表

MRS集群版本	受影响组件
MRS 3.1.1	Hive、Oozie、Flink、Ranger、Tez
MRS 3.1.0	Hive、Flink、Spark、Tez、Impala、Ranger、Presto、Oozie
MRS 3.0.5	Hive、Flink、Spark、Tez、Impala、Ranger、Presto、Oozie、Storm、Loader
MRS 3.0.2	Hive、Flink、Spark、Tez、Ranger、Oozie、Storm、Loader
MRS 2.1.1	Hive、Tez、Storm、Loader、Impala、Presto
MRS 2.1.0	Loader、Hive、Storm、Presto、Impala、Tez、Spark、HBase
MRS 1.9.3	Loader、Hive、Tez、Spark、Flink
MRS 1.9.2	Loader、Hive、Tez、Spark、Flink、Impala

MRS集群版本	受影响组件
MRS 1.9.0	Loader、Hive、Spark、Flink
MRS 1.8.10	Loader、Storm
MRS 1.7.1	Loader、Storm

1.2 MRS Fastjson 漏洞修复指导

1.2.1 简介

问题描述

Fastjson披露存在一处反序列化远程代码执行漏洞，漏洞影响所有1.2.80及以下版本，成功利用漏洞可绕过autoType限制，实现远程任意执行代码。

影响风险

存在漏洞的业务被攻击时，将可能导致攻击者远程在业务平台中执行任意代码。

预防与建议

在产品未发布对应解决方案前，建议您参考以下的相关预防措施。

1. 加固物理设备安全边界，防止外网直接访问及攻击内网管理平面。
2. 排查平台各组件节点是否使用默认密码，如果有，建议修改新密码。
3. 加强环境管理面账户密码管控，确保不泄露不扩散。
4. 部分安全厂商已经提供了针对该漏洞的预防措施，您可联系对应的安全厂商，通过在安全设备上设置拦截规则来预防此类攻击。

1.2.2 影响范围

涉及版本

MRS 3.x

涉及模块

- 管理面：不涉及该漏洞
- 租户面：Manager（Web+Controller+nodeagent）、Kafka、Flink、Redis

说明

- MRS 3.1.0.x执行以下章节：
  - **修复Manager Web**
  - **修复Manager Controller**
  - **修复Manager nodeagent**
- MRS 3.1.2.x执行章节：
  - **修复Manager Web**
  - **修复Manager Controller**
  - **修复Manager nodeagent**
  - **修复Kafka**
  - **修复Flink**

1.2.3 修复 Manager Web

前提条件

已获取FusionInsight Manager登录地址及admin帐号。

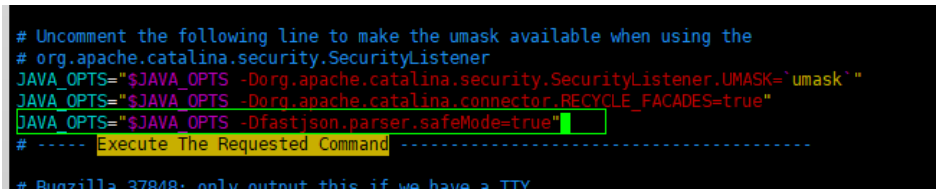
操作步骤

步骤1 使用**omm**用户登录到主OMS节点，备份“$OM_TOMCAT_HOME/bin/catalina.sh”文件。

cp $OM_TOMCAT_HOME/bin/catalina.sh /tmp

步骤2 执行命令**vi $OM_TOMCAT_HOME/bin/catalina.sh**，找到“Execute The Requested Command”所在行，在该行上面添加一行新内容：

```
JAVA_OPTS="$JAVA_OPTS -Dfastjson.parser.safeMode=true"
```



步骤3 使用**omm**用户在主OMS节点执行如下命令重启Manager Web 服务。

$OMS_RUN_PATH/workspace/ha/module/harm/plugin/script/tomcat stop

$OMS_RUN_PATH/workspace/ha/module/harm/plugin/script/tomcat start

步骤4 在主OMS节点查看进程：

ps -ef |grep tomcat | grep om-server

如果包含参数“-Dfastjson.parser.safeMode=true”，说明漏洞问题已经规避，如下图所示：

步骤5 使用**omm**用户在备OMS节点同样执行**1**与**2**。

----结束

1.2.4 修复 Manager Controller

前提条件

已获取FusionInsight Manager登录地址及admin帐号。

操作步骤

步骤1 使用**omm**用户登录到主OMS节点，备份**$CONTROLLER_HOME/sbin/controller.sh**文件。

cp $CONTROLLER_HOME/sbin/controller.sh /tmp

步骤2 执行命令**vi $CONTROLLER_HOME/sbin/controller.sh**，找到JVM_ARGS=所在行，在该行的下一行添加一行新内容：

```
JVM_ARGS="$JVM_ARGS -Dfastjson.parser.safeMode=true"
```

步骤3 使用**omm**用户在主OMS节点执行如下命令重启Controller 服务。

sh /opt/Bigdata/om-server/om/sbin/restart-controller.sh

步骤4 在主OMS节点查看进程。

ps -ef |grep ControllerService

如果包含参数“ -Dfastjson.parser.safeMode=true”，说明漏洞问题已经规避，如下图所示：

步骤5 使用**omm**用户在备OMS节点重复执行**1**与**2**。

----结束

1.2.5 修复 Manager nodeagent

前提条件

已获取FusionInsight Manager登录地址及admin帐号。

操作步骤

步骤1 使用**omm**用户登录到主OMS节点，备份**$NODE_AGENT_HOME/bin/nodeagent_ctl.sh**文件。

cp $NODE_AGENT_HOME/bin/nodeagent_ctl.sh /tmp

步骤2 执行命令**vi $NODE_AGENT_HOME/bin/nodeagent_ctl.sh**，找到“JVM_ARGS=”所在行，在该行的下一行添加一行新内容：


```
JVM_ARGS="$JVM_ARGS -Dfastjson.parser.safeMode=true"
```

步骤3 在集群所有节点执行1和2。

可以手动通过**omm**用户将修改好的“$NODE_AGENT_HOME/bin/nodeagent_ctl.sh”文件覆盖到所有节点。

步骤4 使用**omm**用户在主OMS节点执行如下命令重启集群所有节点NodeAgent。

$CONTROLLER_HOME/inst/restartAllNoes.sh

步骤5 登录集群后台节点查看进程：

ps -ef |grep NodeAgent

如果包含参数“-Dfastjson.parser.safeMode=true”，说明漏洞问题已经规避，如下图所示：

----结束

1.2.6 修复 Kafka

前提条件

已获取FusionInsight Manager登录地址及admin帐号。

操作步骤

步骤1 登录FusionInsight Manager页面，选择“集群 > 服务 > Kafka > 配置 > 全部配置”，搜索参数“KAFKAUI_HEAP_OPTS”。在参数值中添加“ -Dfastjson.parser.safeMode=true”（注意与前参数有空格），如下所示：

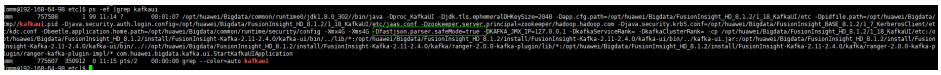
例如原参数值为：“-Xmx4G -Xms4G”，则修改后的参数值为：“-Xmx4G -Xms4G -Dfastjson.parser.safeMode=true”。

步骤2 单击“保存”，配置保存完成后。在Kafka实例页签勾选所有“KafkaUI”实例，选择“更多 > 重启实例”。

步骤3 使用**omm**用户登录任意KafkaUI实例节点，查看进程：

ps -ef | grep KafkaUI

如果包含参数“-Dfastjson.parser.safeMode=true”，说明漏洞问题已经规避，如下所示：



----结束

1.2.7 修复 Flink

前提条件

已获取FusionInsight Manager登录地址及admin帐号。

操作步骤

步骤1 登录FusionInsight Manager页面，选择“集群 > 服务 > Flink > 配置 > 全部配置”，搜索参数“FLINK_SERVER_GC_OPTS”，在该参数值中添加“ -Dfastjson.parser.safeMode=true”（注意与前参数有空格），如下所示：

例如原参数值为：“*xxx*”，则修改后的参数值为：“*xxx* -Dfastjson.parser.safeMode=true”。

步骤2 单击“保存”，配置保存完成后。在Flink实例页签勾选所有“FlinkServer”实例，选择“更多 > 重启实例”。

步骤3 使用**omm**用户登录任意FlinkServe实例节点，查看进程：

ps -ef | grep FlinkServer

如果包含参数“-Dfastjson.parser.safeMode=true”，说明漏洞问题已经规避，如下所示：

----结束

